Front. Comput. Sci., 2025, 19(3): 193802
https://doi.org/10.1007/s11704-024-3542-1

RESEARCH ARTICLE

Incentive mechanism design via smart contract in blockchain-based edge-assisted crowdsensing

Chenhao YING[1,2], Haiming JIN[1], Jie LI[1,2], Xueming SI[1,2], Yuan LUO (✉)[1,2]

1 Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
2 Shanghai Jiao Tong University (Wuxi) Blockchain Advanced Research Center, Wuxi 214101, China

Abstract Edge-assisted mobile crowdsensing (EMCS) has gained significant attention as a data collection paradigm. However, existing incentive mechanisms in EMCS systems rely on centralized platforms, making them impractical for the decentralized nature of EMCS systems. To address this limitation, we propose CHASER, an incentive mechanism designed for blockchain-based EMCS (BEMCS) systems. In fact, CHASER can attract more participants by satisfying the incentive requirements of budget balance, double-side truthfulness, double-side individual rationality and also high social welfare. Furthermore, the proposed BEMCS system with CHASER in smart contracts guarantees the data confidentiality by utilizing an asymmetric encryption scheme, and the anonymity of participants by applying the zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK). This also restrains the malicious behaviors of participants. Finally, most simulations show that the social welfare of CHASER is increased by approximately when compared with the state-of-the-art approaches. Moreover, CHASER achieves a competitive ratio of approximately 0.8 and high task completion rate of over 0.8 in large-scale systems. These findings highlight the robustness and desirable performance of CHASER as an incentive mechanism within the BEMCS system.

Keywords mobile crowdsensing, edge computing, blockchain, smart contract, incentive mechanism

1 Introduction

Recently, the concept of mobile crowdsensing (MCS) has gained significant attention since it was introduced by Jeff Howe in 2006. This approach has been embraced by numerous well-known companies as an efficient paradigm for addressing practical problems. As a result, a plethora of MCS applications have emerged, including notable platforms such as Amazon Mchanical Turk, UBER, Upwork.

A typical mobile crowdsensing (MCS) system comprises a centralized platform, task demanders, and workers. In this system, demanders publish tasks through the platform, which are then executed by the workers. While MCS has seen widespread adoption, it often faces challenges such as network congestion and high latency. These issues arise due to the extensive data processing operations and frequent communication between the centralized platform and the workers. To address these challenges, researchers have proposed edge-assisted MCS (EMCS) systems [1] that incorporate mobile edge computing (MEC). These systems aim to reduce latency and congestion by offloading certain operations from the centralized platform to edge nodes. These edge nodes include devices like smartphones, base stations, laptops, and tablets, each equipped with computing capabilities. By leveraging these edge resources, EMCS systems distribute the computational workload and improve the overall system performance. As a result, EMCS systems are being increasingly employed across various domains [2] to address the limitations of traditional MCS systems.

In an EMCS system, the completion of tasks relies on the quantity and engagement of recruited workers. However, individuals may find participating in an EMCS system costly in terms of time consumption and energy waste. Therefore, it is crucial to design an incentive mechanism within the EMCS system to attract high-quality workers. Although some incentive mechanism designs have been proposed, there are still several problems that need to be addressed due to the limitations of traditional EMCS architecture. First, the traditional EMCS architecture relies on a centralized platform, which inherently suffers from a single point of failure. This means that if the centralized platform experiences an outage or failure, the entire system is affected. For example, in April 2015, Uber China faced a platform outage due to hardware failures, resulting in passengers being unable to cancel their orders. This highlights the vulnerability of centralized architectures and the need for more robust and resilient systems. Second, EMCS systems store sensitive information about demanders and workers, posing risks of privacy breaches and data loss. For instance, there have been cases where famous MCS platforms such as Freelancer have been reported for breaching privacy regulations, exposing user identities. Protecting sensitive information is crucial to

Received July 7, 2023; accepted January 4, 2024

E-mail: yuanluo@sjtu.edu.cn

maintain user trust and ensure data security within EMCS systems. Third, in EMCS systems, both demanders and workers seek to maximize their own benefits, which can lead to conflicts and a phenomenon known as "false reporting." False reporting occurs when workers provide inaccurate or misleading information to gain economic advantages. This behavior can result in higher costs for workers, lower revenue for demanders, and ultimately, a decrease in overall social welfare-the overall benefit of the entire system.

A multitude of incentive mechanisms have been proposed in EMCS systems to tackle the aforementioned challenges. These mechanisms encompass various approaches, such as the utilization of differential privacy and encryption techniques to safeguard data privacy, the implementation of reputation-based systems to combat false reporting, and the adoption of distributed mechanisms to mitigate the risks associated with single point failures. However, it is important to note that, as of now, no existing work has successfully resolved all of these issues simultaneously. While significant progress has been made in each individual area, achieving a comprehensive solution that addresses all aspects remains an ongoing endeavor.

Blockchain is widely recognized as a highly promising architecture for addressing the aforementioned challenges comprehensively. Functioning as a decentralized ledger [3], it is maintained and replicated by all participants in the network. Utilizing a peer-to-peer (P2P) network, blockchain ensures secure, transparent, and decentralized recording of transactions [4]. It offers essential features such as security, data confidentiality, and participant anonymity. Data confidentiality is safeguarded through encryption schemes such as symmetric and asymmetric encryption, while participant anonymity is ensured via zero-knowledge proofs. Transparency is achieved by storing all transactions in blocks, which are verified by the network through a consensus protocol. Additionally, the introduction of smart contracts, initially implemented by Ethereum in 2014, enables the execution of complex transactions within the blockchain. As a result, a compelling question arises: Can we design an incentive mechanism in a blockchain-based EMCS (BEMCS) system that combines security, reliability, and high economic benefits?

However, some new challenges need to be addressed when designing an incentive mechanism in BEMCS system.

First, in the context of designing an incentive mechanism within a blockchain-based system, ensuring participant anonymity through zero-knowledge proofs[5] poses challenges due to the large number of transactions that must be processed promptly. However, traditional zero-knowledge proofs involve back-and-forth message exchanges between the prover and verifier, causing significant delays. To overcome this obstacle, this paper proposes the utilization of an anonymous authentication approach using zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) [6]. zk-SNARK offers several advantages in anonymizing data demanders and workers. First, it enables zero-knowledge proofs, allowing the prover to demonstrate possession of specific information without revealing the information itself. Second, it is succinct, meaning that the proof can be verified within a few milliseconds as the proof length is typically only a few hundred bytes. Third, it is non-interactive, requiring only a single message from the prover to the verifier. Finally, while the proofs of zk-SNARK do not strictly conform to traditional definitions, they effectively serve the same purpose, hence referred to as arguments. The properties of zk-SNARK, particularly its non-interactive nature, significantly enhance the efficiency of the system. By utilizing zk-SNARK in the incentive mechanism design, the paper aims to address the challenge of participant anonymity in a more efficient manner, given the demanding processing requirements of large-scale transaction volumes.

Second, the absence of a trustworthy platform poses challenges in incentivizing greater participation by ensuring truthfulness and individual rationality, two fundamental characteristics of an effective incentive mechanism. While some works in traditional MCS systems have addressed these properties, few have been able to provide them within a blockchain-based system. To address this gap, this paper proposes a probability-based incentive mechanism, wherein demanders and workers are paired based on a threshold determined by probabilistic rules. This mechanism aims to ensure truthfulness and individual rationality within the blockchain-based system, thus facilitating increased participation and engagement.

Third, as mentioned earlier, achieving high economic benefits in a BEMCS system presents challenges. The anonymity of participants and the confidentiality of data make it difficult to address issues such as fake tasks from demanders and waste data submissions from workers. Consequently, the efficiency and economic performance of the BEMCS system are compromised. While some existing works have considered economic properties like worker cost and demander revenue when designing incentive mechanisms in BEMCS systems, none have taken into account the concept of social welfare. Social welfare represents the overall benefit of the entire system, encompassing factors such as worker cost, demander revenue, and the system's overall efficiency. By considering social welfare, the proposed mechanism in this paper offers superior economic performance compared to approaches that only focus on worker cost and demander revenue separately. To achieve high social welfare, this paper introduces a probabilistic model that assumes the random arrival of demanders and workers. This approach aims to enhance the efficiency and economic outcomes of the BEMCS system, ensuring a more equitable distribution of benefits and overall system optimization.

Therefore, after overcoming the above new challenges, we propose a novel incentive mechanism in BEMCS systems utilizing the smart contracts, namely, CHASER. The main contributions of this paper are as follows.

- Mechanism: In Algorithms 1−9, a novel incentive mechanism is proposed, namely, CHASER, applying smart contracts (Algorithms 7−9) after building on a BEMCS system (Algorithms 1−6). In fact, CHASER is based on a probabilistic model where it assumes that all

workers and demanders arrive in a random order. To the best of our knowledge, although there are many incentive mechanisms in the blockchain-based MEC networks [7] and the blockchain-based MCS systems [8], CHASER is the first mechanism in BEMCS and has a more complicated design since it needs to consider the properties of the blockchain, MEC and MCS together.

- Social welfare: Theorem 2 proves that CHASER is $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta})$ competitive on social welfare, where η is a ratio parameter. Although many other works [9] have also investigated the social welfare, the works focusing on its maximization are still missing from the view of theoretical analysis in the BEMCS systems. Furthermore, when η is large, $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta})>1-\frac{1}{e}$, where $1-\frac{1}{e}$ is the best result in many single-side incentive mechanisms.
- Incentive properties: As demonstrated in Theorem 1, CHASER addresses the crucial incentive requirements within BEMCS systems by satisfying the conditions of double-side truthfulness (Lemma 1), double-side individual rationality (Lemma 2) and budget balance (Lemma 3). These lemmas provide strong foundations for attracting participants and ensuring their active involvement in the BEMCS system. By fulfilling these incentive criteria, CHASER promotes a fair and mutually beneficial environment, fostering trust and encouraging widespread participation among both demanders and workers.
- Security properties: Theorem 3 demonstrates that the integration of CHASER in smart contracts within the BEMCS system ensures data confidentiality through the implementation of an asymmetric encryption scheme. Additionally, it provides anonymity for data demanders and workers by utilizing an anonymous authentication approach based on zk-SNARK. This not only protects sensitive information but also serves as a deterrent against malicious behaviors from participants. By incorporating these security measures, the BEMCS system with CHASER establishes a robust and trustworthy environment, safeguarding data privacy and fostering a more reliable and secure crowdsensing ecosystem.
- Evaluations: Extensive simulations are performed to evaluate the performance of CHASER. The results show that CHASER achieves a remarkable increase of approximately 42% in social welfare compared to state-of-the-art approaches. This indicates the superior overall benefit and efficiency that CHASER brings to the BEMCS system. Furthermore, the simulation results demonstrate that CHASER achieves a competitive ratio of approximately 0.8 in certain scenarios. This signifies the effectiveness and competitiveness of CHASER in delivering favorable outcomes for both demanders and workers within the BEMCS system. Moreover, CHASER maintains a task completion rate over 0.8 in large-scale systems. This highlights the robustness and scalability of CHASER in ensuring a high level of task completion within the BEMCS system. The simulation findings validate the effectiveness and practicality of CHASER, showcasing its superior performance compared to the existing approaches.

The rest of this paper is organized as follows. Section 2 introduces some works that related to this paper. Section 3 illustrates the preliminaries. The design details of the proposed mechanism is shown in Section 4 and the theoretical analysis of the mechanism is presented in Section 5. Finally, the performance evaluation is shown in Section 6, after which, Section 7 concludes the whole paper.

2 Related works in blockchain

This section presents an overview of existing works that are relevant to the subject matter of this paper.

2.1 Incentive mechanism in traditional MCS system

Recently, numerous incentive mechanisms have emerged with the goal of attracting more participants to engage in executing outsourced tasks. Some notable works in this area have focused on optimizing the revenue of workers or the platform itself. For instance, Karaliopoulos et al. [10] investigated the maximization of worker contributions to various tasks, considering the bounded rationality of workers. Li et al. [11] formulated worker attraction as a utility optimization problem and developed an incentive mechanism based on contract theory, demonstrating the attainment of Nash Equilibrium among workers' strategies. However, all these workers are built in the traditional MCS system whose implementation depends on a trustworthy platform. Additionally, Wang et al. [12] designed privacy-preserving mechanisms to safeguard users' bid information from the honest-but-curious platform while minimizing the social cost associated with winner selection. Nonetheless, these mechanisms were designed for centralized MCS systems, which are susceptible to the single point of failure issue mentioned earlier. Xiao et al. [13] investigated the incentive mechanism design in MCS systems that take the freshness of collected data and social benefits into concerns. Sun et al. [14] proposed a novel cooperative multi-objective multi-agent reinforcement learning framework to serve as the first preference-configurable order dispatch mechanism for hire-vehicle-enabled crowd sensing platforms.

2.2 Blockchain in mobile crowdsensing

Numerous works have explored the integration of blockchain technology into MCS systems. Li et al. [15] introduced a decentralized framework that eliminates the need for a trusted third-party platform, enabling mobile workers to execute sensing tasks. Chen et al. [16] focused on an enhanced authentication and data transmission scheme, which is verified by formal security proofs and informal security analysis. An et al. [17] propopsed a blockchain-based framework for data quality in edge-computing-enabled crowdsensing. Yu et al. [18] proposed a reputation management scheme utilizing blockchain to identify and handle malicious workers. Zhang et al. [19] also presented a secure framework that combines cryptographic techniques with blockchain advancements. Additionally, Zhang et al. [20] proposed a novel reliable

vehicular MCS system that employed a blockchain oracle to protect participant privacy, along with a unique vehicular data aggregation mechanism to preserve data privacy. However, it is important to note that only a few of these works considered participant anonymity and the economic performance of the system. An et al. [17] proposed a blockchain-based framework for data quality in edge-computing-enabled crowdsensing. Mukkamala et al. [21] proposed a blockchain-based decentralized truth discovery scheme for crowdsourcing with computation integrity guarantees against malicious participants. Yuan et al. [22] introduced a scheme that promotes collaborative edge training between edge servers by introducing incentives and trust based on blockchain. Wang et al. [23] proposed a triple real-time trajectory privacy protection mechanism based on edge computing and blockchain.

2.3 Blockchain in mobile edge computing

Numerous authors have extensively researched the integration of blockchain in MEC. Hao et al. [24] presented an inspection policy based on zero-sum game theory and a roadside unit incentive mechanism jointly using contract theory and subjective logic model. Feng et al. [25] introduced an optimization scheme to balance the performance of blockchain and MEC in blockchain-enabled MEC systems. Sun et al. [26] developed a double auction mechanism in blockchain-based MEC, taking into account both resource allocation and incentive requirements. Xiao et al. [27] presented a blockchain-driven scheme to prevent faked service attacks in MEC. Utilizing a Stackelberg dynamic game, Xu et al. [28] designed a resource trading mechanism for the MEC resource allocation. Jin et al. [29] formulated a non-linear time-varying integer program that jointly places blockchain nodes and determines the number of training iterations to minimize the long-term blockchain computation and communication cost. Amiri et al. [30] presented a permissioned blockchain system designed specifically for edge computing networks. Yuan et al. [31] proposed a novel blockchain-based decentralized platform, to drive and support cooperative multi-access edge computing.

However, these works did not delve into the aspect of attracting more participants to actively engage in the system, which remains an important consideration.

3 Background and preliminaries

This section introduces the system overview, incentive model, cryptographic preliminaries, and securiy requirement respectively.

3.1 System overview

A BEMCS system consists of the following parts.

- **Demander:** A set $\mathcal{D} = \{d_1, \ldots, d_m\}$ of data demanders, where each demander d_i has a sensing task τ_i requiring to be solved.
- **Worker:** A set $\mathcal{W} = \{w_1, \ldots, w_n\}$ of workers, where each worker w_ℓ can be allocated to a demander to execute sensing tasks.
- **Edge node:** A set $\mathcal{E} = \{e_1, \ldots, e_k\}$ of edge nodes, where each edge node e_j verifies the proof provided by the demander or the worker and also proposes a new block (mining). They are selected by algorithms according to their reputation or other rules, where these algorithms are out of the scope of this paper.
- **Smart contract (SC):** It includes a set of codes that enable the allocation of demanders' tasks to workers. These codes are designed in such a way that once they are posted, they cannot be modified or altered.
- **Blockchain oracle (BO):** It is an oracle machine that retrieves external sensory data collected by the workers within blockchain networks.
- **Registration authority (RA):** The workers, demanders, edge nodes, and BO register at the registration authority, enabling them to actively participate in the blockchain networks.

Figure 1 shows the workflow of CHASER with the following illustration.

- Step 1: Each participant, including the demander, worker, edge node, and BO, completes the registration process at RA and receives a unique certificate (Step 1).
- Steps 2−4: The demander d_i initiates the publication of a sensing task τ_i, including relevant information such as her bidding value b_i^d and deposit B_i^d, to the SC (Step 2). The submitted task is then verified by the edge nodes (Step 3), who validate the authenticity and correctness of the task. Once verified, the edge nodes propose a new block that includes the transaction for the verified sensing task (Step 4).
- Steps 5−6: The worker submits her information to SC (Step 5) including her deposit B_ℓ^w and bidding price b_ℓ^w for executing the task. The submitted information is then verified by the edge nodes (Step 6), who ensure authenticity and correctness of information.
- Step 7: The SC obtains winning worker set $\mathcal{S}_\mathcal{W}$, and winning demander set $\mathcal{S}_\mathcal{D}$. Moreover, it obtains the match (d_i, w_ℓ), which means that task τ_i of $d_i \in \mathcal{S}_\mathcal{D}$ will be executed by $w_\ell \in \mathcal{S}_\mathcal{W}$. Furthermore, the payment p_i^d charged to demander $d_i \in \mathcal{S}_\mathcal{D}$, and the payment p_ℓ^w to worker $w_\ell \in \mathcal{S}_\mathcal{W}$ are also obtained (Step 7).
- Steps 8−10: The worker w_ℓ submits the encrypted data to the blockchain via the BO (Step 8), which is then transferred to demander d_i (Step 9). The SC charges p_i^d to the winning demander d_i and pays p_ℓ^w to the winning worker w_ℓ (Step 10) if the exchange is validated.

3.2 Problem statement and motivation

Traditional centralized MCS system relies on a trusted platform, which in practice leads to many problems, such as the single point failure, privacy leakage and data loss. Therefore, to overcome these obstacles, some decentralized MCS system have been built on blockchain by utilizing the decentralized structure and the security property of blockchain. However, as a decentralized system, blockchain-based MCS system requires to incentivize more participants to take part in the sensing tasks. However, participating in the

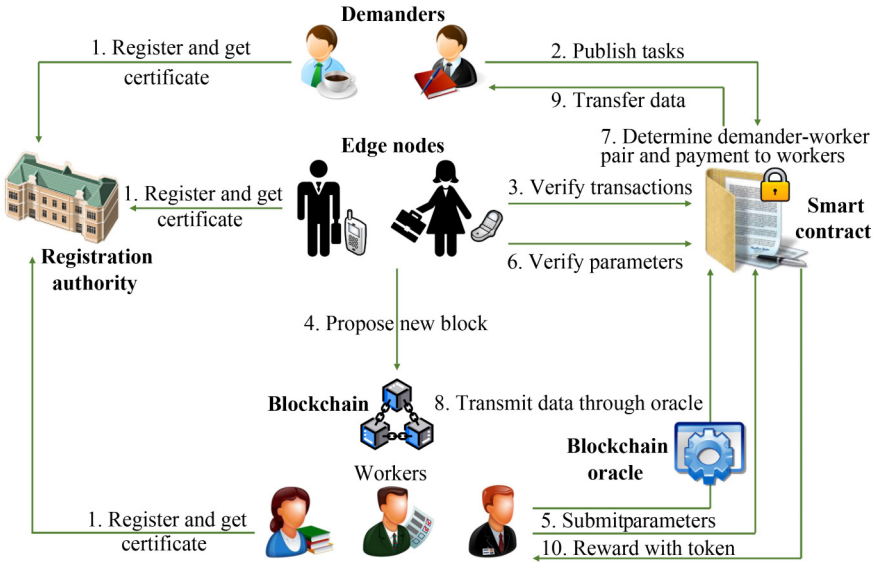

Fig. 1 Framework of CHASER, where the numbers represent the order of events

blockchain-based MCS system is more costly for individuals compared with that of traditional MCS system since apart from the sensing tasks, it requires to consume resources in other aspects, such as the block mining (transaction verifying). Therefore, it is necessary to design an incentive mechanism to attract more participation. However, designing an incentive mechanism in blockchain-based MCS system requires to solve some new problems that are the investigating target of this paper.

- **High economic benefits:** As an incentive mechanism, it requires to follow three basic properties, namely, the truthfulness, the individual rationality, and the budget balance, which are defined in Definitions 1, 2, and 3, respectively. Furthermore, we also aim to design a mechanism that can guarantee a high social benefit and low social cost. Therefore, considering them together, this paper will pursue a high social welfare defined in Definition 4.
- **Strong participant anonymity:** In the practical outsourcing application, all participants, who publish or execute sensing tasks, require to register with their private information such as name, age, and address. To overcome the information leakage, this paper will allow the incentive mechanism to guarantee the participant anonymity by utilizing the zk-snark introduced in Section 3.4.
- **Efficient data security:** Finally, since the data collected by workers usually involves their sensitive information, submitting the data in the decentralized system will leakage the privacy. Therefore, the final target of this paper is to guarantee the security of submitting data by utilizing asymmetric encryption introduced in Section 3.4.

In one word, this paper aim to design a blockchain-based incentive mechanism that guarantees the high economic benefit, strong participant anonymity, and efficient data security.

3.3 Incentive model in smart contract

To address the reluctance of individuals to join in BEMCS systems due to the associated costs, an incentive model is implemented. This model aims to attract strategic and self-interested participants by offering them incentives for their participation. By providing rewards or benefits, the incentive model encourages individuals to actively engage in the BEMCS system, overcoming their reservations about the associated costs and motivating them to contribute their resources, time, and efforts to the tasks at hand.

When denoting the actual value of $d_i \in \mathcal{D}$ as v_i from the executed task τ_i and the actual cost of $w_\ell \in \mathcal{W}$ as c_ℓ, the corresponding utility of d_i is

$$u_i^d = \begin{cases} v_i - p_i^d, & \text{if } d_i \in \mathcal{S}_\mathcal{D}, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

and the corresponding utility of w_ℓ is

$$u_\ell^w = \begin{cases} p_\ell^w - c_\ell, & \text{if } w_\ell \in \mathcal{S}_\mathcal{W}, \\ 0, & \text{otherwise}. \end{cases} \tag{2}$$

In the incentive mechanism proposed in this paper, the main focus is on the transaction fee as the primary source of reward for edge nodes (miners) in the blockchain system. The transaction fee, which is paid by the corresponding demander for publishing a sensing task, serves as a key incentive to motivate edge nodes to validate and include the transaction in a block. For the transaction fee, it is paid by SC, which is denoted as

$$u_j^e = \sum_{(d_i,w_\ell)\in\mathcal{S}_{\mathcal{D}\times\mathcal{W}}} \frac{1}{|\mathcal{E}_{i,\ell}|}(p_i^d - p_\ell^w - \epsilon), \tag{3}$$

where $\mathcal{E}_{i,\ell}$ with the cardinality $|\mathcal{E}_{i,\ell}|$ is the set of edge nodes whose vote is consistent to the final decision in the blockchain system for the transaction between demander d_i and worker w_ℓ. Furthermore, $\epsilon \geqslant 0$ is a constant satisfying $\epsilon < p_i^d - p_\ell^w$.

Additionally, the utility of smart contract is

$$u_0 = \sum_{d_i \in \mathcal{S}_\mathcal{D}} p_i^d - \sum_{w_\ell \in \mathcal{S}_\mathcal{W}} p_\ell^w - \sum_{e_j \in \mathcal{E}} u_j^e. \quad (4)$$

It is important to note that this paper does not specifically address the block reward, which is a separate form of reward paid by the blockchain system itself. Instead, the primary emphasis is on the transaction fee as a component of the incentive model within the BEMCS system. Furthermore, as shown in Eq. (3), it is observed that the gas cost associated with the mining operation by the edge node e_j is not considered. This omission is deliberate, as the gas cost is inherently dependent on the operational mechanism of the underlying blockchain system, rather than the incentive mechanism itself. Consequently, the exclusion of the gas cost does not impact the implementation of the incentive mechanism, as the mechanism can be implemented once the blockchain system is functioning normally.

It is an important consideration that executing smart contracts in a blockchain system typically incurs a gas cost, which is predetermined during the compilation of the smart contract. As the gas cost can be known in advance, it is possible to include the corresponding gas in the bids submitted by demanders. By doing so, the reported bid value from a demander already accounts for the gas cost, effectively removing the need to separately consider the gas cost when designing an auction-based incentive mechanism. Therefore, in the context of the proposed auction-based incentive mechanism, the gas cost is implicitly incorporated within the bids, and there is no need to explicitly factor it in as a separate component during the mechanism's design.

Due to the selfish and strategic nature of workers and demanders, a demander d_i may send a bid b_i^d that is different from the actual value v_i to maximize her utility. Similarly, a worker w_ℓ may send a bid b_ℓ^w that is different from the actual cost c_ℓ. This problem can be overcome by the truthfulness of the incentive model.

Definition 1 [Truthfulness] An incentive model is double-side truthful if for sensing task τ_i, the actual consumed cost c_ℓ of worker w_ℓ and actual obtained value v_i of demander d_i maximize their utilities, respectively.

Note that the "**Truthfulness**" and the "**Truthful**" mentioned in this paper are both from the incentive requirements rather than the security requirements. Another desirable property to attract the participation is the individual rationality.

Definition 2 [Individual Rationality] An incentive mechanism satisfies the double-side individual rationality if the utilities of demander d_i and worker w_ℓ are $u_i^d \geqslant 0$ and $u_\ell^w \geqslant 0$, respectively.

Additionally, the budget balance is another property that needs to be satisfied by an appropriate incentive model, which is defined as follows.

Definition 3 [Budget Balance] An incentive model satisfies the budget balance if for each pair of winning worker $w_\ell \in \mathcal{S}_\mathcal{W}$ and demander $d_i \in \mathcal{S}_\mathcal{D}$, where the task τ_i of d_i is executed by w_ℓ, the utility of SC is non-negative.

Apart from the above three properties, an excellent incentive model can also achieve a high social welfare defined as follows.

Definition 4 [Social Welfare] The social welfare of a BEMCS system is defined as

$$\begin{aligned}\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}}) &= u_0 + \sum_{d_i \in \mathcal{D}} u_i^d + \sum_{w_\ell \in \mathcal{W}} u_\ell^w + \sum_{e_j \in \mathcal{E}} u_j^e \\ &= \sum_{d_i \in \mathcal{S}_\mathcal{D}} v_i - \sum_{w_\ell \in \mathcal{S}_\mathcal{W}} c_\ell, \end{aligned} \quad (5)$$

where $\mathcal{S}_{\mathcal{D}\times\mathcal{W}} = \{(d_i, w_\ell) \in \mathcal{S}_\mathcal{D} \times \mathcal{S}_\mathcal{W} \mid$ task τ_i of demander d_i is executed by worker $w_\ell\}$. Eq. (5) illustrates that the social welfare in this paper accounts for the utilities of the SC, workers, and demanders, as well as the transaction fee. While the social welfare formula includes four components, it is primarily influenced by the benefits of demanders and the costs of workers. It is worth noting that the block reward and the gas cost of edge nodes do impact the overall social welfare. However, since these factors are determined by the underlying blockchain networks and are outside the scope of the incentive mechanism being investigated in this paper, they are not explicitly considered in the analysis of social welfare. By disregarding the block reward and gas cost in the incentive model, this paper aims to provide a comprehensive analysis of the economic aspects of the system, focusing specifically on the participant-level utilities and overall social welfare that can be influenced by the proposed incentive mechanism.

3.4 Cryptographic preliminaries

This paper employs zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) [6] as an anonymous authentication mechanism to anonymize data demanders and workers. To construct zk-SNARKs, a suitable characterization of the complexity class NP is selected. NP-complete problems, such as the circuit satisfiability (Circ-SAT) problem, are often used in the construction of zk-SNARK schemes. These problems provide a solid foundation for building zk-SNARKs for NP-complete languages, enabling the anonymous authentication of participants in the blockchain-based EMCS system described in this paper. For convenience, let's define the NP-complete language to establish the zk-SNARK as $\mathcal{L} = \{x | \exists \omega, \text{s.t.}, C(x, \omega) = 1\}$. Therefore, the proving algorithm of zk-SNARK can generate a proof to attest a statement $x \in \mathcal{L}$ with help of private witness ω, where the proof can be efficiently checked by verifying algorithm of zk-SNARK. Informally, zk-SNARK employed in Algorithms 2–5 is a tuple $(\mathsf{KeyGen}, \mathsf{Prove}, \mathsf{Verify})$ of polynomial-time algorithm:

- $\mathsf{KeyGen}(1^\lambda) \to (\mathsf{pp}, \mathsf{td})$. Inputting a security parameter λ where 1^λ means the all ones vector with length λ, the key generator $\mathsf{KeyGen}(\cdot)$ of zk-SNARK obtains a public parameter pp and a trapdoor td, where pp will be broadcasted for proving and verifying the membership in language $\mathcal{L}$ introduced in Section 4.
- $\mathsf{Prove}(\mathsf{pp}, x, \omega) \to \pi$. Inputting the above public parameter pp, private witness ω and public knowledge x, a non-interaction proof π is obtained by the prover

$\mathsf{Prove}(\cdot)$ for the statement $x \in \mathcal{L}$.

- $\mathsf{Verify}(\mathsf{pp}, x, \pi) \to b$. Inputting the proof π, public knowledge x, and public parameter pp, if $x \in \mathcal{L}$ is validated, the verifier $\mathsf{Verify}(\cdot)$ outputs $b = 1$.

A digital signature scheme [32] is a fundamental cryptographic technique that provides authentication, integrity, and non-repudiation for digital messages or documents. It plays a crucial role in ensuring the security and trustworthiness of communication in various domains. In a digital signature scheme, a signer uses their private key to generate a unique signature for a specific message or document. This signature serves as a cryptographic proof of authenticity and integrity. The signer then attaches the digital signature to the message or document and sends it to the recipient. To verify the digital signature, the recipient utilizes the signer's public key, which is freely available. By applying a verification algorithm, the recipient can validate the signature, ensuring that the message originated from the claimed sender and has not been tampered with during transmission. In the context of BEMCS system in this paper, the incorporation of digital signature schemes enhances the overall security and trustworthiness of the system. It enables participants to establish the authenticity and integrity of messages, facilitating secure communication and reliable transactions. A digital signature scheme $\mathsf{Sig} = (\mathcal{G}_{\mathsf{sig}}, \mathcal{K}_{\mathsf{sig}}, \mathcal{S}_{\mathsf{sig}}, \mathcal{V}_{\mathsf{sig}})$ is applied in Algorithms 2−5.

- $\mathcal{G}_{\mathsf{sig}}(1^{\lambda}) \to \mathsf{pp}_{\mathsf{sig}}$. Utilizing a security parameter λ, the public parameters $\mathsf{pp}_{\mathsf{sig}}$ are sampled by $\mathcal{G}_{\mathsf{sig}}(\cdot)$ for the digital signature scheme.
- $\mathcal{K}_{\mathsf{sig}}(\mathsf{pp}_{\mathsf{sig}}) \to (\mathsf{pk}_{\mathsf{sig}}, \mathsf{sk}_{\mathsf{sig}})$. Utilizing the public parameters $\mathsf{pp}_{\mathsf{sig}}$, a public-secret key pair $(\mathsf{pk}_{\mathsf{sig}}, \mathsf{sk}_{\mathsf{sig}})$ is sampled by $\mathcal{K}_{\mathsf{sig}}(\cdot)$.
- $\mathcal{S}_{\mathsf{sig}}(\mathsf{sk}_{\mathsf{sig}}, m) \to \sigma$. Inputting the secret key $\mathsf{sk}_{\mathsf{sig}}$ and a message m, a signature σ of message m is obtained by utilizing $\mathcal{S}_{\mathsf{sig}}(\cdot)$.
- $\mathcal{V}_{\mathsf{sig}}(\mathsf{pk}_{\mathsf{sig}}, m, \sigma) \to b$. Inputting the signature σ, message m and public key $\mathsf{pk}_{\mathsf{sig}}$, $b = 1$ is outputted by $\mathcal{V}_{\mathsf{sig}}(\cdot)$ if the signature σ is valid, otherwise $b = 0$.

Public-key encryption [32], also known as asymmetric encryption, is a fundamental cryptographic technique that facilitates secure communication and data protection in various applications. It operates using a pair of mathematically related keys: a public key and a private key. In a public-key encryption scheme, the sender employs the recipient's public key to encrypt the message, ensuring that only the intended recipient, possessing the corresponding private key, can decrypt it. This process guarantees confidentiality and privacy, as the encrypted message remains indecipherable to unauthorized entities. The utilization of public-key encryption schemes holds significant importance in the secure functioning of the BEMCS system proposed in this paper. It facilitates secure communication among participants, safeguards sensitive data, and ensures the integrity and authenticity of messages and transactions. A public-key encryption scheme $\mathsf{Enc} = (\mathcal{G}_{\mathsf{enc}}, \mathcal{K}_{\mathsf{enc}}, \mathcal{E}_{\mathsf{enc}}, \mathcal{D}_{\mathsf{enc}})$ is applied in Algorithm 4.

- $\mathcal{G}_{\mathsf{enc}}(1^{\lambda}) \to \mathsf{pp}_{\mathsf{enc}}$. Utilizing a security parameter λ, the public parameters $\mathsf{pp}_{\mathsf{enc}}$ are sampled by $\mathcal{G}_{\mathsf{enc}}(\cdot)$ for the asymmetric encryption scheme.
- $\mathcal{K}_{\mathsf{enc}}(\mathsf{pp}_{\mathsf{enc}}) \to (\mathsf{pk}_{\mathsf{enc}}, \mathsf{sk}_{\mathsf{enc}})$. Utilizing the public parameters $\mathsf{pp}_{\mathsf{enc}}$, a public-secret key pair $(\mathsf{pk}_{\mathsf{enc}}, \mathsf{sk}_{\mathsf{enc}})$ is sampled by $\mathcal{K}_{\mathsf{enc}}(\cdot)$.
- $\mathcal{E}_{\mathsf{enc}}(\mathsf{pk}_{\mathsf{enc}}, m) \to c$. Inputting a message m and public key $\mathsf{pk}_{\mathsf{enc}}$, a ciphertext c of message m is obtained by utilizing $\mathcal{E}_{\mathsf{enc}}(\cdot)$.
- $\mathcal{D}_{\mathsf{enc}}(\mathsf{sk}_{\mathsf{enc}}, c) \to m$. Inputting the ciphertext c and secret key $\mathsf{sk}_{\mathsf{enc}}$, the message m is outputted by $\mathcal{D}_{\mathsf{enc}}(\cdot)$.

By leveraging the zk-SNARK, signature scheme, and public-key encryption scheme, it is possible to establish an effective anonymity authentication scheme. This scheme is designed to provide authentication guarantees while preserving the anonymity of participants.

- $\mathcal{G}_{\mathsf{auth}}(1^{\lambda}) \to \mathsf{pp}$. Utilizing a security parameter λ, the public parameters pp are sampled by $\mathcal{G}_{\mathsf{auth}}(\cdot)$ for authenticate scheme with zk-SNARK. In fact, the parameter λ is also used to generate a key pair $(\mathsf{cpk}_{\mathsf{sig}}, \mathsf{csk}_{\mathsf{sig}})$ by RA for a digital signature scheme.
- $\mathsf{Auth}(\mathsf{pp}, p\|m, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{sk}^i_{\mathsf{sig}}, \mathsf{pk}^i_{\mathsf{sig}}, \sigma_i)$: Under the input message $p\|m$ with prefix p, the algorithm fist computes two tags $t_1 = \mathsf{CRH}(p, \mathsf{sk}^i_{\mathsf{sig}})$ and $t_2 = \mathsf{CRH}(p\|m, \mathsf{sk}^i_{\mathsf{sig}})$, where $\mathsf{CRH}(\cdot)$ is a secure hash function. Then, let $x = (p\|m, \mathsf{cpk}_{\mathsf{sig}})$ be the common knowledge, and $\omega = (\mathsf{sk}^i_{\mathsf{sig}}, \mathsf{pk}^i_{\mathsf{sig}}, \sigma_i)$ be the private witness, after which, the algorithm runs the proving algorithm $\mathsf{Prove}(\mathsf{pp}, x, \omega)$ of zk-SNARK for the language $\mathcal{L} = \{x = (p\|m, \mathsf{cpk}_{\mathsf{sig}}) | \exists\, \omega = (\mathsf{sk}^i_{\mathsf{sig}}, \mathsf{pk}^i_{\mathsf{sig}}, \sigma_i), \text{s.t.}, \mathcal{V}_{\mathsf{sig}}(\mathsf{cpk}_{\mathsf{sig}}, \mathsf{pk}^i_{\mathsf{sig}}, \sigma_i) = 1 \&\& \mathsf{Pair}(\mathsf{pk}^i_{\mathsf{sig}}, \mathsf{sk}^i_{\mathsf{sig}}) = 1 \&\& t_1 = \mathsf{CRH}(p, \mathsf{sk}^i_{\mathsf{sig}}) \&\& t_2 = \mathsf{CRH}(p\|m, \mathsf{sk}^i_{\mathsf{sig}})\}$, where $\mathsf{Pair}(\cdot)$ is to verify whether two keys belongs to the identical public-secret key pair, whose output is 1 if they are consistent, and 0 otherwise. $\mathsf{Prove}(\cdot)$ obtains a proof η_i for $x \in \mathcal{L}$. $\mathsf{Auth}(\cdot)$ then outputs $\pi_i = (t_1, t_2, \eta_i)$.
- $\mathsf{Vefy}(p\|m, \mathsf{pp}, x, \pi) \to b$. Inputting the proof π, public knowledge x, and public parameter pp, it runs the verifying algorithm of zk-SNARK and outputs decision $d \in \{0, 1\}$.

3.5 Security requirement in BEMCS

As previously discussed, the design of incentive mechanisms in traditional MCS and EMCS systems often encounters significant challenges, with privacy disclosure being a primary concern. Participants in these systems prioritize two aspects of privacy security: data confidentiality and anonymity. To provide a formal understanding of these security requirements, we present the following definitions.

Definition 5 [Data Confidentiality] Data confidentiality is a set of rules or a promise that limits access or places restrictions on any information that is being shared. In other words, it refers to protection of data from unauthorized access and disclosure, including means for protecting personal privacy and proprietary information.

During the implementation of the BEMCS system, it is important to ensure the privacy and security of the communication transcripts. This includes the sensory data submitted by workers, as well as the proofs generated by demanders and workers utilizing zk-SNARK (zero-knowledge succinct non-interactive arguments of knowledge). The objective is to prevent any leakage of information to unauthorized parties.

Definition 6 [Anonymity] Anonymity is a state of being unidentified in any process of possession, transfer, or creation of information. The identity can't be disclosed to anyone except the person who owns this identity or represents it.

To ensure anonymity in the BEMCS system, it is crucial to prevent the linking of demanders and workers, thereby safeguarding their private information from adversaries. Anonymity necessitates that participants cannot be easily associated with their actions or identities during task execution. This protection against linkage by adversaries is vital to protect the privacy and confidentiality of participants' information. By implementing appropriate measures, the system can ensure that participants remain anonymous and their identities are not compromised.

In the context of the BEMCS system, it is acknowledged that participants may have incentives to report false information to maximize their own utility. This paper specifically addresses the issue of false reporting attacks, as the selection of workers and demanders in the system is based on auctions where participants are chosen according to their reported bids. In addition to emphasizing data confidentiality and anonymity, this research focuses on mitigating the negative impact of false reporting attacks, as these deceptive bids can significantly harm the system's integrity and performance. To establish a clear understanding, the definition for false reporting is provided.

Definition 7 [False Bid Attack] It includes two cases:

- A malicious demander may report a false bid that is lower than her actual revenue such that she can offer less payment to workers.
- A malicious worker may report a false bid that is high than her actual cost such that she can obtain more reward from demanders.

According to the false bid attack, we define the security against the malicious participants.

Definition 8 [Security against the malicious participants] A malicious participant $\mathcal{M}$ corrupts a demander or worker, and participates in the protocol. The security means that the happening probability of false bid attack launched by$\mathcal{M}$ is negligibly small.

In fact, due to the security against malicious participants, all participants obtain the actual utility according to their contribution, which improves the robustness of the system.

4 Illustration of proposed framework

In this section, the BEMCS system is built first, after which the design details of CHASER are shown. Finally, an example is presented to illustrate the workflow of CHASER. Note that the description of BEMCS focuses on the procedures atop the blockchain. It means the operations underlying the blockchain infrastructure are omitted.

4.1 Details of the BEMCS system

This subsection shows the details of BEMCS systems whose outlines are presented in Algorithms 1−6, respectively, with six corresponding paragraphs, where Algorithm 1 corresponds to Step 1 in Section 3.1 and Algorithm 2 to Steps 2−4, while Algorithm 3 corresponds to Steps 5−6 and Algorithms 4−6 to Steps 8−10. Note that CHASER is also one phase of BEMCS systems, whose details are presented in the next subsection.

1. Registration for the In-chain participants: RA generates a public-secret key pair ($\mathsf{cpk}_{\mathsf{sig}}$, $\mathsf{csk}_{\mathsf{sig}}$) for the certification and a public parameter pp for zk-SNARK, after which it broadcasts $\mathsf{cpk}_{\mathsf{sig}}$ and pp. Then, each arrived participant creates a public-secret key pair ($\mathsf{pk}_{\mathsf{sig}}, \mathsf{sk}_{\mathsf{sig}}$) for the signature and registers with RA, after which, the participant, gets a certificate σ from RA to bind the public key $\mathsf{pk}_{\mathsf{sig}}$ and her ID by utilizing the secret key $\mathsf{csk}_{\mathsf{sig}}$. Finally, each participant needs to deposit some tokens B, e.g., demander d_i deposits B_i^d. For convenience, we add some distinct letters (d, w, e) in the parameter to distinguish different roles. For example, the public-secret key pair of demander d_i is ($\mathsf{dpk}_{\mathsf{sig}}^i, \mathsf{dsk}_{\mathsf{sig}}^i$).

2. Task publishing by utilizing the zk-SNARK:

- Operation of demanders: When a sensing task τ_i needs to be executed, demander d_i generates a new account address α_i^d. She writes the information $\mathsf{INFO}_i = (b_i^d, B_i^d, \mathsf{dpk}_{\mathsf{enc}}^i, \pi_i^d)$, including a bidding value b_i^d, a deposit B_i^d, a public key $\mathsf{dpk}_{\mathsf{enc}}^i$, as well as an attestation $\pi_i^d = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_i^d, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{dsk}_{\mathsf{sig}}^i, \mathsf{dpk}_{\mathsf{sig}}^i, \sigma_i^d)$, to authenticate the inputting message $\alpha \| \alpha_i^d$, where the attestation π_i^d means that demander d_i really holds a secret key with valid certificate. The steps of $\mathsf{Auth}(\cdot)$ is introduced in Section 3. Finally, the transaction $\mathcal{T}_i$ with INFO_i is sent to SC via the one-task-only address α_i^d.
- Operation of edge nodes: After observing the transaction $\mathcal{T}_i$ of demander d_i, each edge node e_j verifies and votes utilizing $\mathbf{V}_j^{d_i} = \mathsf{Vefy}(\mathsf{pp}, \pi_i^d, \alpha \| \alpha_i^d, \mathsf{cpk}_{\mathsf{sig}})$, where $\mathsf{Vefy}(\cdot)$ is shown in Section 3. The vote is sent to SC via its address α_j^e. Note that the consensus

Algorithm 1 Registration for the in-chain participants

Input: The security parameter λ.
Output: The public parameter pp, certificate and public-secret key pair of each participant for the signature.

RA computes $\mathsf{pp} = \mathsf{KeyGen}(1^\lambda)$ and $(\mathsf{cpk}_{\mathsf{sig}}, \mathsf{csk}_{\mathsf{sig}}) = \mathcal{K}_{\mathsf{sig}}(\mathsf{pp}_{\mathsf{sig}})$, after which, it broadcasts pp and $\mathsf{cpk}_{\mathsf{sig}}$;
for *each participant* **do**
  Compute $\mathsf{pp}_{\mathsf{sig}} = \mathcal{G}_{\mathsf{sig}}(1^\lambda)$;
  Get $(\mathsf{pk}_{\mathsf{sig}}, \mathsf{sk}_{\mathsf{sig}})$ and σ and deposit some tokens B, e.g., demander d_i deposits B_i^d and worker w_ℓ for B_ℓ^w. For convenience, we add some distinct letters (d, w, e) in the parameter to distinguish different roles. For example, the a public-secret key pair of demander d_i is $(\mathsf{dpk}_{\mathsf{sig}}^i, \mathsf{dsk}_{\mathsf{sig}}^i)$ and certificate σ_i^d.

Algorithm 2 Task publishing by utilizing the zk-SNARK

Input: The outputs of Algorithm 1, security parameter λ, and information of task τ_i, i.e., the bidding value b_i^d, and the deposit B_i^d.
Output: A new proposed block.
// **Operations of Demanders:**
for *each arrived demander* d_i **do**
  Compute an address α_i^d for sending the information;
  Get $\pi_i^d = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_i^d, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{dsk}_{\mathsf{sig}}^i, \mathsf{dpk}_{\mathsf{sig}}^i, \sigma_i^d)$, where α is the address of the SC;
  Get $\mathsf{INFO}_i = (b_i^d, B_i^d, \mathsf{dpk}_{\mathsf{enc}}^i, \pi_i^d)$, write into the transaction $\mathcal{T}_i$ and send $\mathcal{T}_i$ to the SC via the address α_i^d;
// **Operations of Edge Nodes:**
for *each edge node* e_j **do**
  Compute $\mathbf{V}_j^{d_i} = \mathsf{Vefy}(\mathsf{pp}, \pi_i^d, \alpha \| \alpha_i^d, \mathsf{cpk}_{\mathsf{sig}})$ and send to SC via its address α_j^e;
// **Operations of SC:**
if $\mathbf{V}^{d_i} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{d_i} \geqslant \beta$ *where* β *is a parameter* **then**
  Go to **CHASER**;

algorithm can be the practical Byzantine fault tolerance (PBFT) and delegated proof of stake (DPoS), whose design is out the scope of this work.

- Operations of SC: The transaction $\mathcal{T}_i$ is validated once $\mathbf{V}^{d_i} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{d_i} \geqslant \beta$, where β is a parameter, after which, the algorithm goes to CHASER.

3. Parameter submission utilizing the zk-SNARK: After observing the block, workers submit their parameters.

- Operation of workers: When a worker w_ℓ arrives to execute the sensing task, she also generates a one-task-only address α_ℓ^w. Then, she writes a parameter list $\mathsf{PARM}_\ell = (b_\ell^w, B_\ell^w, \pi_\ell^w)$ including her bidding price b_ℓ^w and deposit B_ℓ^w as well as an attestation $\pi_\ell^w = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_\ell^w, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{wsk}_{\mathsf{sig}}^\ell, \mathsf{wpk}_{\mathsf{sig}}^\ell, \sigma_\ell^w)$ to authenticate the inputting message $\alpha \| \alpha_\ell^w$, where the attestation π_ℓ^w means that worker w_ℓ really holds a secret key with valid certificate. Finally, PARM_ℓ is sent to SC applying the address α_ℓ^w.
- Operation of edge nodes: Similar to the Taks Publishing shown in Algorithm 2, after observing the parameters of workers, edge node e_j verifies and votes.
- Operations of SC: The algorithm then goes to CHASER to determine the winning worker set $\mathcal{S}_\mathcal{W}$ and winning demander set $\mathcal{S}_\mathcal{D}$, as well as the corresponding payments. The details of CHASER are illustrated in the next subsection.

Algorithm 3 Parameter submi ssion utilizing zk-SNARK

Input: The outputs of Algorithm 1 and the deposit B_ℓ^w of each worker w_ℓ.
Output: The PARM_ℓ of each worker.
// **Operations of Workers:**
for *each arrived worker* w_ℓ **do**
  Compute an address α_ℓ^w for sending the parameters and the collected data;
  Get $\pi_\ell^w = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_\ell^w, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{wsk}_{\mathsf{sig}}^\ell, \mathsf{wpk}_{\mathsf{sig}}^\ell, \sigma_\ell^w)$;
  Write $\mathsf{PARM}_\ell = (b_\ell^w, B_\ell^w, \pi_\ell^w)$ and send PARM_ℓ to the SC utilizing the address α_ℓ^w;
// **Operations of Edge Nodes:**
for *each edge node* e_j **do**
  Compute $\mathbf{V}_j^{w_\ell} = \mathsf{Vefy}(\mathsf{pp}, \pi_\ell^w, \alpha \| \alpha_\ell^w, \mathsf{cpk}_{\mathsf{sig}})$ and send to SC via the address α_j^e;
// **Operations of SC:**
if $\mathbf{V}^{w_\ell} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{w_\ell} \geqslant \beta$ **then**
  Go to **CHASER**;

Algorithm 4 Data collection utilizing asymmetric encryption

Input: The outputs of Algorithms 1 and 8 as well as the sensory data $\mathcal{D}_\ell$ of each winning worker w_ℓ.
Output: The signed ciphertext C_ℓ.
// **Operation of Workers:**
for *each worker* $w_\ell \in \mathcal{S}_\mathcal{W}$ **do**
  Compute $C_\ell = \mathcal{E}_{\mathsf{enc}}(\mathsf{dpk}_{\mathsf{enc}}^i, \mathcal{D}_\ell)$;
  Compute $\bar{\pi}_\ell^w = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_\ell^w \| C_\ell, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{wsk}_{\mathsf{sig}}^\ell, \mathsf{wpk}_{\mathsf{sig}}^\ell, \sigma_\ell^w)$;
  Send C_ℓ and $\bar{\pi}_\ell^w$ uses the address α_ℓ to blockchain network via BO;
// **Operations of Edge Nodes:**
for *each edge node* e_j **do**
  Compute $\mathbf{V}^{w_\ell} = \mathsf{Vefy}(\mathsf{pp}, \bar{\pi}_\ell^w, \alpha \| \alpha_\ell^w \| C_\ell, \mathsf{cpk}_{\mathsf{sig}})$ to check whether C_ℓ is the first submission and send to SC;
// **Operation of SC:**
if $\mathbf{V}^{w_\ell} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{w_\ell} \leqslant \beta$ **then**
  Send B_ℓ^w to demander d_i and drop the data C_ℓ;
else
  Go to Algorithm 5;

4. Data collection utilizing asymmetric encryption: Finishing CHASER, SC broadcasts the winner sets $\mathcal{S}_\mathcal{W}$, $\mathcal{S}_\mathcal{D}$, and match $\mathcal{S}_{\mathcal{D}\times\mathcal{W}}$ as well as the payments p_i^d and p_ℓ^w charged to the demanders and paid to the workers, respectively.

- Operation of workers: After receiving the corresponding information, worker $w_\ell \in \mathcal{S}_\mathcal{W}$ encrypts the sensory data $\mathcal{D}_\ell$ to obtain the ciphertext C_ℓ utilizing the public key $\mathsf{dpk}_{\mathsf{enc}}^i$ of demander d_i and computes $\bar{\pi}_\ell^w = \mathsf{Auth}(\mathsf{pp}, \alpha \| \alpha_\ell^w \| C_\ell, \mathsf{cpk}_{\mathsf{sig}}, \mathsf{wsk}_{\mathsf{sig}}^\ell, \mathsf{wpk}_{\mathsf{sig}}^\ell, \sigma_\ell^w)$. Then, the encrypted data C_ℓ and attestation $\bar{\pi}_\ell^w$ are sent to blockchain via BO. The truth of data $\mathcal{D}_\ell$ is verified by an attestation service.
- Operation of edge nodes: After receiving the proofs, each edge node e_j computes the vote $\mathbf{V}^{w_\ell} = \mathsf{Vefy}(\mathsf{pp}, \bar{\pi}_\ell^w, \alpha \| \alpha_\ell^w \| C_\ell, \mathsf{cpk}_{\mathsf{sig}})$ to check whether C_ℓ is the first submission.
- Operation of SC: If $\mathbf{V}^{w_\ell} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{w_\ell} \leqslant \beta$, SC sends B_ℓ^w to demander d_i and drops the data C_ℓ, otherwise, it goes to Algorithm 5. It says that the encrypted data is sent to the network via BO. Alghough BO is trustworthy, it

Algorithm 5 Payment transferring after the verification

Input: The outputs of Algorithms 4.
Output: The transfer is completed.
// **Operations of Demanders and SC:**
for *each demander* $d_i \in \mathcal{S}_\mathcal{D}$ *observes the SC to obtain* C_ℓ **do**
  Decrypts C_ℓ to obtain data $\mathcal{D}_\ell$;
  Compute $\bar{\pi}_i^d = \mathsf{Prove}(\mathsf{pp}, (R_\ell, \mathsf{INFO}_i), \mathsf{dsk}_{\mathsf{enc}}^i)$;
  Put $\bar{R}$ and $\bar{\pi}_i^d$ into a block transaction and send the block to the blockchain network;
// **Operations of Edge Nodes:**
for *each edge node* e_j **do**
  Compute $\mathbf{V}_j^{d_i} = \mathsf{Verify}(\mathsf{pp}, \bar{\pi}_i^d, (R_\ell, \mathsf{INFO}_i))$ and send it to SC;
// **Operations of SC:**
if $\mathbf{V}^{d_i} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{d_i} \geqslant \beta$ **then**
  Pay $B_\ell^w + p_\ell^w$ to worker w_ℓ, where $p_\ell^w = \bar{c}$, and refund $B_i^d - p_i^d$ to demander d_i, where $p_i^d = \bar{v}$;
else
  Pay B_i^d to worekr w_ℓ;

may also manipulate the data transmitted to demanders. Therefore, the TLSNotary is used to provide the proof of validity. Furthermore, the data transmitted by BO can be optionally saved on a decentralized storage system such as Swarm or IPFS.

5. Payment transferring after the verification: After demander d_i receives the encrypted data C_ℓ, the BEMCS systems work as follows.

- Operation of demanders: demander d_i decrypts to obtain the data $\mathcal{D}_\ell$ and computes $\bar{\pi}_i^d = \mathsf{Prove}(\mathsf{pp}, (R_\ell, \mathsf{INFO}_i), \mathsf{dsk}_{\mathsf{enc}}^i)$, with the secret key $\mathsf{dsk}_{\mathsf{enc}}^i$ as the witness to attest the validation of her reward instruction, where the proof is for the NP-Language $\mathcal{L} = \{x = (R_\ell, \mathsf{INFO}_i) | \exists \omega = (\mathsf{dsk}_{\mathsf{enc}}^i, \mathsf{dpk}_{\mathsf{enc}}^i)$, s.t., $\mathsf{D}_\ell = \mathcal{D}_{\mathsf{enc}}(\mathsf{dsk}_{\mathsf{enc}}^i, C_\ell) \&\& R_\ell = R(\mathcal{W}, \mathcal{D}) \&\& \mathsf{Pair}(\mathsf{dsk}_{\mathsf{enc}}^i, \mathsf{dpk}_{\mathsf{enc}}^i) = 1\}$, where $R_\ell = R(\mathcal{W}\backslash\{w_\ell\}, \mathcal{D}\backslash\{d_i\})$ is the reward instruction to worker w_ℓ.
- Operation of Edge nodes: After receiving the proofs, each edge node e_j computes the vote $\mathbf{V}_j^{d_i} = \mathsf{Verify}(\mathsf{pp}, \bar{\pi}_i^d, (R_\ell, \mathsf{INFO}_i))$ and sends it to SC.
- Operation of SC: If the vote $\mathbf{V}^{d_i} = \sum_{e_j \in \mathcal{E}} \mathbf{V}_j^{d_i} \geqslant \beta$, SC sends $B_\ell^w + p_\ell^w$ to worker w_ℓ and refunds $B_i^d - p_i^d$ to demander d_i, otherwise, it sends B_i^d to worker w_ℓ.

6. Reward and penalty for the edge nodes: To incentivize edge nodes to participate in the verification process, the proposed approach in this paper offers a reward of $\frac{1}{|\mathcal{E}_{i,\ell}|}(p_i^d - p_\ell^w - \epsilon)$ to each edge node e_j, where p_i^d is the payment charged to demander d_i and p_ℓ^w is the fee paid to worker w_ℓ. Furthermore, $\epsilon \geqslant 0$ is a constant set by SC satisfying $\epsilon < p_i^d - p_\ell^w$ and $\mathcal{E}_{i,\ell}$ is the set of edge nodes with cardinality $|\mathcal{E}_{i,\ell}|$ who have the positive vote. This reward is granted if the votes of the edge node align with the final decision. However, if an edge node's vote deviates from the final decision, they will receive no reward as a form of punishment. It is worth noting that the paper assumes the edge nodes to be honest, implying that they will only make faulty votes if their computational power is insufficient. However, the system can also leverage the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm to handle adversarial edge nodes. PBFT enables consensus among the edge nodes as long as the number of adversarial nodes remains below one-third of the total number of nodes.

In the BEMCS system, edge nodes receive rewards comprising the block reward and the transaction fee, where the former is provided by the blockchain network (such as Ethereum) and the latter is paid by the demanders. However, it is important to note that Algorithm 6 in the paper specifically focuses on the transaction fee as the described reward, while the block reward is not considered as it relies on the operation mechanism of the blockchain system (e.g., Ethereum or Bitcoin) rather than the proposed incentive mechanism. Additionally, the costs incurred by edge nodes for participating in the blockchain system, such as gas fees for mining, are also outside the scope of the paper as they are dependent on the specific blockchain network being utilized. To summarize, the rewards discussed in Algorithm 6 pertain to the transaction fees paid by demanders to incentivize edge nodes within the BEMCS system. The paper does not directly address the block reward or the costs associated with participating in the blockchain system, as those aspects are governed by the operational mechanisms of the underlying blockchain network. Although the paper does not explicitly consider the mining cost in the BEMCS system, it highlights that the CHASER can be implemented whenever the underlying blockchain system is operational.

Algorithm 6 **Reward and penalty for the edge nodes**

Input: The set $\mathcal{E}$ of edge nodes.
Output: The reward or the penalty.
for *each edge node* $e_j \in \mathcal{E}$ *and each task* **do**
  if *Its vote is equal to the final decision* **then**
    Reward e_j with $\frac{1}{|\mathcal{E}_{i,\ell}|}(p_i^d - p_\ell^w - \epsilon)$;
  else
    Reward e_j nothing as the punishment;

Remark 1 Our anonymous protocol mainly focuses on the BEMCS system that is built in the application layer on top of the blockchain infrastructure. The anonymity in network layer is not considered in this paper, but it can be guaranteed by applying some existing works, e.g., Zcash [33]. For convenience, each worker and demander in this paper generates a one-task-only address for each task to support the anonymity in the underlying blockchain.

4.2 Details of CHASER

This subsection presents the details of CHASER. CHASER is our proposed incentive mechanism applied by SC and consists of three phases, namely, Standard Determination, Winner Selection and Payment Determination, whose outlines are shown in Algorithms 7–9. These algorithms correspond to Step 7 in Section 3.1.

7. Standard determination of CHASER: After the information verification, SC works as follows.

- Silent observation: After defining a selection probability $\phi \in (0, 1/2]$, a value L of observation window is drawn by SC according to a binomial distribution $\mathcal{B}(|\mathcal{D}| + |\mathcal{W}|, \phi)$. SC further obtains an observing demander set $\mathcal{D}_L$ and an observing worker set $\mathcal{W}_L$ by seeing the first L arrivals.
- Typical allocation: It then lists the bidding values b_i^d of demanders $d_i \in \mathcal{D}_L$ in decreasing order and lists the bidding prices b_ℓ^w of workers $w_\ell \in \mathcal{W}_L$ in increasing order. The demander d_i with the ith largest bid b_i^d in $\mathcal{D}_L$ and the worker w_i with the i-th least bid b_i^w in $\mathcal{W}_L$ are added to an allocation set $\mathcal{S}^*_{\mathcal{D}_L \times \mathcal{W}_L}$ when $b_i^d \geqslant b_i^w$, where $1 \leqslant i \leqslant L$.
- Standard selection: After defining a ratio parameter $\eta \in (|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$, SC selects the bids of workers and demanders at the location $\lceil (1 - 2\phi^{-1} \cdot \sqrt[3]{\eta}) \cdot |\mathcal{S}^*_{\mathcal{D}_L \times \mathcal{W}_L}| \rceil$ of $\mathcal{S}^*_{\mathcal{D}_L \times \mathcal{W}_L}$ as the standard cost and value, respectively, which are denoted as $\bar{c}$ and $\bar{v}$, where $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ is obtained

Algorithm 7 **Standard determination of CHASER**

Input: The outputs of Algorithm 2.
Output: Standard cost $\bar{c}$ and standard value $\bar{v}$.

Define a *ratio parameter* $\eta \in (|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$ and draw a value L a binomial distribution $\mathcal{B}(|\mathcal{D}|+|\mathcal{W}|, \phi)$, where $\phi \in (0, 1/2]$ is a *selection probability*;
Define an observing worker set $\mathcal{W}_L \leftarrow \emptyset$ and demander set $\mathcal{D}_L \leftarrow \emptyset$, as well as an allocation set $\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L} \leftarrow \emptyset$;
// **Silent Observation:**
for *The i* th *arrival, where* $i \leqslant L$ **do**
  if *It is a demander* d_i **then**
    $\mathcal{D}_L \leftarrow \mathcal{D}_L \cup \{d_i\}$;
  else if *It is a worker* w_i **then**
    $\mathcal{W}_L \leftarrow \mathcal{W}_L \cup \{w_i\}$;
// **Typical Allocation:**
Order the bid b^w_ℓ of $w_\ell \in \mathcal{W}_L$ in an increasing order and bid b^d_i of $d_i \in \mathcal{D}_L$ in a decreasing order;
for *The the i-th least* b^w_i *and the i-th largest* b^d_i*, where* $1 \leqslant i \leqslant \min\{|\mathcal{D}_L|, \mathcal{W}_L|\}$ **do**
  if $b^d_i \geqslant b^w_i$ **then**
    $\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L} \leftarrow \mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L} \cup \{(d_i, w_i)\}$;
// **Standard Selection:**
if $\lceil(1-2\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L}|\rceil \leqslant 0$ **then**
  Set $\bar{c} \leftarrow -\infty$ and $\bar{v} \leftarrow \infty$;
else
  Let $\bar{v}$ and $\bar{c}$ be the bids of the demander and worker at location $\lceil(1-2\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L}|\rceil$ of $\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L}$, respectively;

by applying the Typical Allocation over $\mathcal{D}$ and $\mathcal{W}$.

Remark 2 Algorithm 7 sets two important parameters namely, ratio parameter η and selection probability ϕ, where $\phi \in (0, 1/2]$ and $\eta \in (|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$. For the selection probability η, it is used to draw the size L of observation queue Q from a binomial distribution $\mathcal{B}(|\mathcal{D}|+|\mathcal{W}|, \phi)$. The selection probability ϕ just needs to guarantee that the observation queue Q is not empty. It is observed that for any positive value $\phi \in (0, \frac{1}{2}]$, the condition can be satisfied easily once the number of workers and demanders is not too small. Furthermore, for the ratio parameter η, it is used together with ϕ to determine the standard cost and value by $\lceil(1-2\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L}|\rceil$. To obtain a nontrivial standard cost and value ($\bar{e} \neq -\infty$ and $\bar{c} \neq \infty$), it requires that 1. $\mathcal{S}^*_{\mathcal{D}_L\times\mathcal{W}_L}$ is not empty; 2. $1-2\phi^{-1}\cdot\sqrt[3]{\eta} > 0$. Condition 1 is satisfied once the scale of system is not too small. Furthermore, Condition 2 is satisfied when $\eta < \frac{1}{8}\cdot\phi^3$. This can be achieved easily. For example, ϕ is close to $\frac{1}{2}$ and η is less than $\frac{1}{64}$. Since η is selected in the interval $(|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$, $\eta \leqslant \frac{1}{64}$ can be satisfied when the number of demander-worker pairs is not too small, e.g., it is larger than 100, which can be guaranteed in the practical MCS system such as MTurk. Furthermore, since the values of $\bar{v}$ and $\bar{c}$, which are determined by the parameters η and ϕ, impact the selection of workers and demanders and further influence the task completion rate. Therefore, an appropriate selection of η and ϕ is important. For example, in an ideal situation where the bids of demanders in $\mathcal{W}\backslash\mathcal{D}_L$ are all larger than $\bar{v}$ and the bids of workers in $\mathcal{W}\backslash\mathcal{W}_L$ are all less than $\bar{c}$, when setting $\phi = \frac{1}{5}$ and $\eta = \frac{1}{1000}$, which means that the scale of system is at most larger than 1000, the task completion rate is larger than 80%.

8. Winner selection of CHASER: SC first defines a sequence Q.

Algorithm 8 **Winner selection of CHASER**

Input: The outputs and the inputs of Algorithm 7.
Output: The winning demander set $\mathcal{S}_\mathcal{D}$, the worker set $\mathcal{S}_\mathcal{W}$, and the match $\mathcal{S}_{\mathcal{D}\times\mathcal{W}}$.

Define a sequence $Q \leftarrow \emptyset$ to store the arrivals arrived after the Silent Observation;
Define an alternative demander set $\mathcal{A}^d \leftarrow \emptyset$ and an alternative worker set $\mathcal{A}^w \leftarrow \emptyset$;
for *every arrival after the Silent Observation* **do**
  Add it to the end of Q;
  // **Arrival of Workers:**
  if *a worker* $w_\ell \in \mathcal{W}\backslash\mathcal{W}_L$ *arrives and* $b^w_\ell \leqslant \bar{c}$ **then**
    $\mathcal{A}^w \leftarrow \mathcal{A}^w \cup \{w_\ell\}$;
    if $\mathcal{A}^d \neq \emptyset$ **then**
      Allocate w_ℓ to the earliest arrived demander $d_i \in \mathcal{A}^d$ in Q, *i.e.,* the match is (d_i, w_ℓ);
      $\mathcal{A}^w \leftarrow \mathcal{A}^w\backslash\{w_\ell\}$, $\mathcal{A}^d \leftarrow \mathcal{A}^d\backslash\{d_i\}$, $Q \leftarrow Q\backslash\{d_i, w_\ell\}$;
      $\mathcal{S}_\mathcal{D} \leftarrow \mathcal{S}_\mathcal{D} \cup \{d_i\}$, $\mathcal{S}_\mathcal{W} \leftarrow \mathcal{S}_\mathcal{W} \cup \{w_\ell\}$, $\mathcal{S}_{\mathcal{D}\times\mathcal{W}} \leftarrow \mathcal{S}_{\mathcal{D}\times\mathcal{W}} \cup (d_i, w_\ell)$;
  // **Arrival of Demanders:**
  if *a demander* $d_i \in \mathcal{D}\backslash\mathcal{D}_L$ *arrives and* $b^d_i \geqslant \bar{v}$ **then**
    $\mathcal{A}^d \leftarrow \mathcal{A}^d \cup \{d_i\}$;
    if $\mathcal{A}^w \neq \emptyset$ **then**
      Allocate d_i to the earliest arrived worker $w_\ell \in \mathcal{A}^w$ in Q, *i.e.,* the match is (d_i, w_ℓ);
      $\mathcal{A}^w \leftarrow \mathcal{A}^w\backslash\{w_\ell\}$, $\mathcal{A}^d \leftarrow \mathcal{A}^d\backslash\{d_i\}$, $Q \leftarrow Q\backslash\{d_i, w_\ell\}$;
      $\mathcal{S}_\mathcal{D} \leftarrow \mathcal{S}_\mathcal{D} \cup \{d_i\}$, $\mathcal{S}_\mathcal{W} \leftarrow \mathcal{S}_\mathcal{W} \cup \{w_\ell\}$, $\mathcal{S}_{\mathcal{D}\times\mathcal{W}} \leftarrow \mathcal{S}_{\mathcal{D}\times\mathcal{W}} \cup (d_i, w_\ell)$;

- Arrival of workers: When a worker $w_\ell \in \mathcal{W}\backslash\mathcal{W}_L$ arrives, SC adds her to an alternative worker set $\mathcal{A}^w$ if her bidding price $b^w_\ell \leqslant \bar{c}$. Furthermore, worker w_ℓ is allocated to the earliest arrived demander $d_i \in \mathcal{A}^d$ in the sequence Q if the a set $\mathcal{A}^d$ is not empty.
- Arrival of demanders: When the arrival is a demander $d_i \in \mathcal{D}\backslash\mathcal{D}_L$, she is added to an alternative demander set $\mathcal{A}^d$ if her bidding value $b^d_i \geqslant \bar{v}$. Similarly, demander d_i is allocated to the earliest arrived worker $w_\ell \in \mathcal{A}^w$ if $\mathcal{A}^w \neq \emptyset$.

9. Payment determination of CHASER: SC determines the corresponding payments.

- Payment from demanders: The payment charged to winning demander $d_i \in \mathcal{S}_\mathcal{D}$ is $p^d_i = \bar{v}$.
- Payment to workers: The payment to winning worker $w_\ell \in \mathcal{S}_\mathcal{W}$ is $p^w_\ell = \bar{c}$.

Finally, an example is shown to illustrate the workflow of CHASER, i.e., Algorithms 7, 8, and 9.

Example 1 There are seven demanders $\mathcal{D} = \{d_1, d_2, d_3, d_4, d_5, d_6, d_7\}$ with the tasks $\{\tau_1, \tau_2, \tau_3, \tau_4, \tau_5, \tau_6, \tau_7\}$ and bids $\{b^d_1 = 3.8, b^d_2 = 2.6, b^d_3 = 3.2, b^d_4 = 3.3, b^d_5 = 4.6, b^d_6 = 2.7, b^d_7 =$

Algorithm 9 **Payment determination of CHASER**

Input: The outputs of Algorithms 7 and 8.
Output: The payment p^d_i charged to each demander $d_i \in \mathcal{S}_\mathcal{D}$, the payment p^w_ℓ to each worker $w_\ell \in \mathcal{S}_\mathcal{W}$.

// **Payment Charged to Demanders:**
for *every* $d_i \in \mathcal{S}_\mathcal{D}$ **do**
  $p^d_i \leftarrow \bar{v}$;
// **Payment to Workers:**
for *every* $w_\ell \in \mathcal{S}_\mathcal{W}$ **do**
  $p^w_\ell \leftarrow \bar{c}$;

4.1}, as well as six workers $\mathcal{W} = \{w_1, w_2, w_3, w_4, w_5, w_6\}$ with the bids $\{b_1^w = 2.9, b_2^w = 2.1, b_3^w = 3.1, b_4^w = 3.9, b_5^w = 3.3, b_6^w = 2.5\}$. In Standard Determination, according to the binomial distribution $\mathcal{B}(|\mathcal{D}| + |\mathcal{W}|, \phi) = \mathcal{B}(13, 1/2)$ with $\phi = 1/2$, SC obtains a value $L = 8$ and observes the first eight arrivals, which are supposed to be $\{d_1, w_1, w_2, w_3, w_4, d_2, d_3, d_4\}$ in that order. It means that $\mathcal{D}_L = \{d_1, d_2, d_3, d_4\}$ and $\mathcal{W}_L = \{w_1, w_2, w_3, w_4\}$. Since $\min\{|\mathcal{D}_L|, |\mathcal{W}_L|\} = 4$, after four iterations with $\eta = 0.001$, it can be obtained that $\mathcal{S}_{\mathcal{D}_L \times \mathcal{W}_L} = \{(d_1, w_2), (d_4, w_1), (d_3, w_3)\}$. Therefore, since $\lceil (1 - 2\phi^{-1} \cdot \sqrt[3]{\eta}) \cdot |\mathcal{S}^*_{\mathcal{D}_L \times \mathcal{W}_L}| \rceil = 2$, the standard cost and value are $\bar{c} = b_1^w = 2.9$ and $\bar{v} = b_4^d = 3.3$, respectively. In Winner Selection, by assuming the arrival sequence after the Silent Observation is $\mathcal{Q} = \{d_5, d_6, d_7\}$ in that order, the alternative worker set $\mathcal{A}^w$ is empty and the alternative demander set is $\mathcal{A}^d = \{d_5, d_7\}$. After that, workers w_5 and w_6 arrive, which means that $\mathcal{A}^w = \{w_6\}$. Therefore, worker w_6 is selected to solve the sensing task τ_5 of d_5, i.e., $\mathcal{S}_{\mathcal{D}} = \{d_5\}$, $\mathcal{S}_{\mathcal{W}} = \{w_6\}$ and $\mathcal{S}_{\mathcal{D} \times \mathcal{W}} = \{(d_5, w_6)\}$. Finally, Payment Determination is carried out, where the payment charged to d_5 is $p_5^d = \bar{v} = 3.3$ and that paid to w_6 is $p_6^w = \bar{c} = 2.9$.

5 Theoretical analysis

This section shows in Theorem 1 that CHASER meets the incentive requirements of budget balance, double-side individual rationality and double-side truthfulness. Moreover, Theorem 2 shows that CHASER achieves a high social welfare. Finally, Theorem 2 investigates the security property of the proposed BEMCS system.

5.1 Incentive analysis

This subsection investigates the social welfare achieved by CHASER and its incentive properties, which are shown in Theorem 2 and Theorem 1, respectively.

Lemma 1 The CHASER mechanism is strategy-proof, i.e., reporting truthfully their private valuations and incurred costs is a weakly dominant strategy both for the demanders and the workers, respectively.

Proof The proof is only for the workers and that for the demanders can be obtained similarly. When arriving in the Silent Observation of Standard Determination, the workers will not be allocated to any demander, which means that they can not obtain any reward whether the costs are reported truthfully. Therefore, the conclusion is trivial. In the rest of proof, it assumes that the workers arrive after the Silent Observation.

According to the rules of the Winner Selection, when the bidding price b_ℓ^w of worker w_ℓ satisfies $b_\ell^w \geqslant \bar{c}$, she will be allocated to a demander to execute the sensing task, where $\bar{c}$ is the standard cost. Therefore, two cases will be considered.

- The actual cost c_ℓ is $c_\ell > \bar{c}$: When the actual cost c_ℓ is $c_\ell > \bar{c}$, worker w_ℓ may report the bidding price b_w^ℓ satisfying $b_w^\ell < \bar{c}$. However, as the rule of payment shown in the Payment Determination, the reward that each winning worker can obtain is only $\bar{c}$, which means that her utility is negative when the reported bidding price $b_\ell^w < \bar{c}$.
- The actual cost c_ℓ is $c_\ell \leqslant \bar{c}$: When the actual cost c_ℓ is $c_\ell \leqslant \bar{c}$, there are two subcases that need to be considered.
  - The bidding price b_ℓ^w is $b_\ell^w > \bar{c}$: According to the rule of the Winner Selection, worker w_ℓ will not be allocated to any demander, which means that the utility is zero.
  - The bidding price $b_\ell^w \leqslant \bar{c}$: According to the rule, the payment to worker w_ℓ is $\bar{c}$ once she is selected to execute the sensing task. Therefore, $b_\ell^w = c_\ell$.

Combining the above cases, the conclusion holds. □

Lemma 2 CHASER ensures that each worker and demander obtains a non-negative utility, which is the double-side individual rationality of the incentive requirements.

Proof The proof also only considers the workers. The first time that the utility of worker w_ℓ may change is that worker w_ℓ is allocated to a demander, in which the bidding price b_ℓ^w of worker w_ℓ satisfies $b_\ell^w \leqslant \bar{c}$. Furthermore, she will be paid the standard cost $\bar{c}$. Since the bidding price b_ℓ^w is truthfully reported, which means that $b_\ell^w = c_\ell$, where c_ℓ is the actual cost, her utility is $u_\ell^w = p_\ell^w - c_\ell = \bar{c} - b_\ell^w \geqslant 0$. □

Lemma 3 CHASER satisfies the budget balance.

Proof Let's assume that demander d_i is allocated to worker w_ℓ. Therefore, the bidding value b_i^d of demander d_i satisfies $b_i^d \geqslant \bar{v}$, where $\bar{v}$ is the standard value, which means that $\bar{v} \neq \infty$. Similarly, the bidding price b_ℓ^w of worker w_ℓ also satisfies $b_\ell^w \leqslant \bar{c}$, where $\bar{c}$ is the standard cost, which means that $\bar{c} \neq -\infty$. Therefore, the conditions that $\bar{v} \neq \infty$ and $\bar{c} \neq -\infty$ imply that there is a demander d_ι being allocated to a worker w_k in the Typical Allocation of Standard Determination, which means $\bar{v} \geqslant \bar{c}$ due to the rule of the Typical Allocation. Furthermore, the payment p_i^d charged to demander d_i to SC is $p_i^d = \bar{v}$, while the payment p_ℓ^w paid to worker w_ℓ is $p_\ell^w = \bar{c}$. Therefore, the conclusion holds since $\bar{v} \geqslant \bar{c}$. Furthermore, once the task of demander d_i is published and executed by worker w_ℓ, the fee that needs to be paid to each edge node e_j whose vote is consistent to the final decision is $\frac{1}{|\mathcal{E}_{i,\ell}|}(p_i^d - p_\ell^w - \epsilon)$, where $|\mathcal{E}_{i,\ell}|$ is the number of edge nodes for positive voting and $\epsilon \geqslant 0$ satisfies $\epsilon < p_i^d - p_\ell^w$. Therefore, the final utility of SC is $\epsilon \geqslant 0$. □

Combining the above lemmas, the following theorem is obtained. Note that unlike Theorem 1 in [34] where the conclusion is a three-party property, this theorem shows that CHASER is double-side truthful and double-side individually rational.

Theorem 1 CHASER satisfies the incentive requirements of budget balance, double-side truthfulness and double-side individual rationality. In fact,

- **Budget balance:** the utility of SC is non-negative for each sensing task.
- **Double-side truthfulness:** each worker and demander submits the bid truthfully.

- **Double-side rationality:** each worker and demander obtains a non-negative utility.

It will be shown in the following part that CHASER achieves a high social welfare, before which, we need the following proposition that is derived in [35].

Lemma 4 [35] For a worker set $\mathcal{W}$ and a demander set $\mathcal{D}$, the result $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ derived by applying the Typical Allocation in Standard Determination maximizes social welfare among all possible allocations, where $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}} = \{(d_i, w_\ell) \in \mathcal{S}^*_{\mathcal{D}} \times \mathcal{S}^*_{\mathcal{W}} \mid$ worker w_ℓ and demander d_i are matched by the Typical Allocation, where w_ℓ executes the task τ_i of $d_i\}$. $\mathcal{S}^*_{\mathcal{D}}$ and $\mathcal{S}^*_{\mathcal{W}}$ are the corresponding winning demander set and worker set obtained over $\mathcal{D}$ and $\mathcal{W}$, respectively.

It should be pointed out that Lemma 4 means that when applying the corresponding Typical Allocation to the whole system, i.e., $\mathcal{W}$ and $\mathcal{D}$, the matching result $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ has the optimal social welfare. However, Algorithm 7 only applies Typical Allocation to the participants in observation queue to determine the standard value and cost.

To show that CHASER achieves a high social welfare, let $\widetilde{\mathcal{D}}$ and $\widetilde{\mathcal{W}}$ be the sets of demanders and workers at the locations from one to $\lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil$ of $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$, respectively, where the selection probability is $\phi \in (0, 1/2]$ and the ratio parameter is $\eta \in (|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$. Note that Lemmas 5−7 appeared in our previous work [34] without the detailed proofs. In contrast, this paper completes the corresponding proofs.

Lemma 5 [34] For workers $w_\ell \in \widetilde{\mathcal{W}}$ and demanders $d_i \in \widetilde{\mathcal{D}}$,

$$\sum_{d_i\in\widetilde{\mathcal{D}}} v_i - \sum_{w_\ell\in\widetilde{\mathcal{W}}} c_\ell \geqslant (1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}), \tag{6}$$

where v_i is the value of d_i and c_ℓ is the cost of w_ℓ, while ϕ is the selection probability and η is the ratio parameter. Additionally, $\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})$ is the social welfare over the allocation result $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ defined in Lemma 4.

Proof According to the definitions of the demander set $\widetilde{\mathcal{D}}$ and worker set $\widetilde{\mathcal{W}}$, the proof only considers $(1-6\phi^{-1}\cdot\sqrt[3]{\eta}) > 0$. When it is non-positive, the conclusion holds immediately.

Since there are $\lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil$ demanders in $\widetilde{\mathcal{D}}$ with the largest value in $\mathcal{S}^*_{\mathcal{D}}$, the values v_i satisfy

$$\sum_{d_i\in\widetilde{\mathcal{D}}} v_i \geqslant \lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil\cdot\frac{\sum_{d_i\in\mathcal{S}^*_{\mathcal{D}}} v_i}{|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|}, \tag{7}$$

where ϕ is the selection probability and η is the ratio parameter, which are defined in the Standard Determination. Furthermore, $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}} = \{(d_i, w_\ell) \in \mathcal{S}^*_{\mathcal{D}} \times \mathcal{S}^*_{\mathcal{W}} \mid$ worker w_ℓ and demander d_i are matched by the Typical Allocation, where w_ℓ executes the task τ_i of $d_i\}$ is obtained by the Typical Allocation in Standard Determination, in which $\mathcal{S}^*_{\mathcal{D}} \subseteq \mathcal{D}$ and $\mathcal{S}^*_{\mathcal{W}} \subseteq \mathcal{W}$ are the corresponding winning demander set and worker set, respectively. Similarly, since there are $\lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil$ workers in $\widetilde{\mathcal{W}}$ with the least cost among the workers in $\mathcal{S}^*_{\mathcal{W}}$, it can be obtained

$$\sum_{w_\ell\in\widetilde{\mathcal{W}}} c_\ell \leqslant \lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil\cdot\frac{\sum_{w_\ell\in\mathcal{S}^*_{\mathcal{W}}} c_\ell}{|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|}, \tag{8}$$

where c_ℓ is the cost of worker w_ℓ. Combining the two inequalities, it can be obtained

$$\begin{aligned}\sum_{d_i\in\widetilde{\mathcal{D}}} v_i - \sum_{w_\ell\in\widetilde{\mathcal{W}}} c_\ell &\geqslant \lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil\cdot\frac{\sum_{d_i\in\mathcal{S}^*_{\mathcal{D}}} v_i - \sum_{w_\ell\in\mathcal{S}^*_{\mathcal{W}}} c_\ell}{|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|}\\ &\geqslant (1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}),\end{aligned} \tag{9}$$

where $\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})$ is the social welfare of $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$. □

To analyse the social welfare of CHASER, the following lemma is necessary, before which, let's define two sets $\widehat{\mathcal{W}} = \{w_\ell \in \mathcal{W}\backslash\mathcal{W}_L | c_\ell < \bar{c}\}$ and $\widehat{\mathcal{D}} = \{d_i \in \mathcal{D}\backslash\mathcal{D}_L | v_i > \bar{v}\}$ with the random order of the entire sequence of demander/worker incidents. It can be seen that the workers in $\widehat{\mathcal{W}}$ are alternative, which means that all of them can be allocated. Similarly, the demanders in $\widehat{\mathcal{D}}$ are also alternative. Let's define a random variable R drawn from a binomial distribution $\mathcal{B}(|\mathcal{D}\backslash\mathcal{D}_L| + |\mathcal{W}\backslash\mathcal{W}_L|, \min\{16\phi^{-1}\cdot\sqrt[3]{\eta}, 1\})$. Similar to the observed arrivals in the Silent Observation, let $\mathcal{W}_R$ and $\mathcal{D}_R$ be the sets of workers and demanders in the last R arrivals, respectively. Still let $\widetilde{\mathcal{D}}$ and $\widetilde{\mathcal{W}}$ be the sets of demanders and workers at the locations from one to $\lceil(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|\rceil$ of $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$, respectively, where the selection probability is $\phi \in (0, 1/2]$ and the ratio parameter is $\eta \in (|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}, 1]$.

Lemma 6 [34] The event $\mathcal{E}$ that all the following incidents are true will happen with the probability at least $1 - 10e^{-2/\sqrt[3]{\eta}}$:

$$\begin{aligned}&(i)\widetilde{\mathcal{D}}\backslash\mathcal{D}_L \subseteq \widehat{\mathcal{D}} \qquad (ii)\widetilde{\mathcal{W}}\backslash\mathcal{W}_L \subseteq \widehat{\mathcal{W}}\\ &(iii)|\widehat{\mathcal{D}}\backslash\mathcal{D}_R| \leqslant |\widehat{\mathcal{W}}| \qquad (iv)|\widehat{\mathcal{W}}\backslash\mathcal{W}_R| \leqslant |\widehat{\mathcal{D}}|\end{aligned}$$

(v) There exists a value ξ satisfying $c_\ell \leqslant \xi \leqslant v_i$, for any demander $d_i \in \widehat{\mathcal{D}}$ and worker $w_\ell \in \widehat{\mathcal{W}}$.

Proof The conclusion holds by the similar method in [35], whose proof is omitted here. □

Lemma 7 [34] The event $\mathcal{E}$ defined in Lemma 6 implies

$$\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}}) \geqslant \sum_{\substack{d_i\in\widetilde{\mathcal{D}}\\ d_i\notin\mathcal{D}_L\cup\mathcal{D}_R}} [v_i - \xi] + \sum_{\substack{w_\ell\in\widetilde{\mathcal{W}}\\ w_\ell\notin\mathcal{W}_L\cup\mathcal{W}_R}} [\xi - c_\ell], \tag{10}$$

where $\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})$ is the social welfare over the allocation result $\mathcal{S}_{\mathcal{D}\times\mathcal{W}} = \{(d_i, w_\ell) \in \mathcal{S}_{\mathcal{D}} \times \mathcal{S}_{\mathcal{W}} \mid$ worker w_ℓ executes the task τ_i of demander $d_i\}$ achieved by CHASER with the winning demander set $\mathcal{S}_{\mathcal{D}} \subseteq \mathcal{D}$ and winning worker set $\mathcal{S}_{\mathcal{W}} \subseteq \mathcal{W}$. Furthermore, v_i is the value of d_i and c_ℓ is the cost of w_ℓ. Additionally, constant ξ is defined in Lemma 6.

Proof Since given event $\mathcal{E}$, it means $|\widehat{\mathcal{W}}\backslash\mathcal{W}_R| \leqslant |\widehat{\mathcal{D}}|$. Furthermore, it can be seen that CHASER allocates at least $|\widehat{\mathcal{W}}\backslash\mathcal{W}_R|$ workers. Since CHASER allocates the workers in $\mathcal{W}_R$ only after all alternative workers in $\mathcal{W}\backslash(\mathcal{W}_L\cup\mathcal{W}_R)$ are allocated, it can be obtained that all workers in $\widehat{\mathcal{W}}\backslash\mathcal{W}_R$ are allocated under the event $\mathcal{E}$. Furthermore, Lemma 6 means

that given $\mathcal{E}$, all workers in $\widetilde{\mathcal{W}}\backslash\mathcal{W}_L$ belong to $\widehat{\mathcal{W}}$. Therefore, the workers in $\widetilde{\mathcal{W}}\backslash(\mathcal{W}_L\cup\mathcal{W}_R)$ are all allocated. The argument of demanders is similar to that of workers. Finally, the event $\mathcal{E}$ also implies that $c_\ell\leqslant\xi\leqslant v_i$ for every pair (d_i,w_ℓ) of worker $w_\ell\in\widehat{\mathcal{W}}$ and demander $d_i\in\widehat{\mathcal{D}}$.

Under the happening of event $\mathcal{E}$, the contribution of a pair (d_i,w_ℓ) of worker w_ℓ and demander d_i obtained by CHASER to social welfare is $v_i-c_\ell=[v_i-\xi]+[\xi-c_\ell]$. Therefore,

$$\begin{aligned}\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})&=\sum_{(d_i,w_\ell)\in\mathcal{S}_{\mathcal{D}\times\mathcal{W}}}v_i-c_\ell=\sum_{(d_i,w_\ell)\in\mathcal{S}_{\mathcal{D}\times\mathcal{W}}}[v_i-\xi]+[\xi-c_\ell]\\&\geqslant\sum_{\substack{d_i\in\widetilde{D}\\d_i\notin\mathcal{D}_L\cup\mathcal{D}_R}}[v_i-\xi]+\sum_{\substack{w_\ell\in\widetilde{W}\\w_\ell\notin\mathcal{W}_L\cup\mathcal{W}_R}}[\xi-c_\ell],\end{aligned}\tag{11}$$

which is the conclusion. □

Applying Lemmas 5 and 7, the following theorem is obtained, which improves the lower bound of the competitive ratio on social welfare achieved by CHASER compared with Theorem 2 in [34] with the form $(1-15\sqrt[6]{\eta})$.

Theorem 2 For a demander set $\mathcal{D}$ and a worker set $\mathcal{W}$, where each demander $d_i\in\mathcal{D}$ with a value v_i and each worker $w_\ell\in\mathcal{W}$ with a cost c_ℓ arrive according to a uniformly random order, CHASER is at least $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta}-10e^{-2/\sqrt[3]{\eta}})$-competitive on social welfare, where the parameter is $\eta\in(|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1},1]$ and the result $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ is obtained by the Typical Allocation in Standard Determination whose expression is shown in Lemma 4. Furthermore, when $\eta\leqslant 0.1$, $10e^{-2/\sqrt[3]{\eta}}$ can be neglected, which means CHASER is at least approximately $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta})$-competitive.

Proof For a demander set $\mathcal{D}'\subseteq\mathcal{D}$ and a worker set $\mathcal{W}'\subseteq\mathcal{W}$, respectively, let $\mathcal{H}(\mathcal{D}',\mathcal{W}')$ be

$$\mathcal{H}(\mathcal{D}',\mathcal{W}')=\sum_{d_i\in\widetilde{\mathcal{D}}\backslash\mathcal{D}'}[v_i-\xi]+\sum_{w_\ell\in\widetilde{\mathcal{W}}\backslash\mathcal{W}'}[\xi-c_\ell].\tag{12}$$

The definition of ξ guarantees that $v_i-\xi\geqslant 0$ and $\xi-c_\ell\geqslant 0$ for every demander $d_i\in\widetilde{\mathcal{D}}\subseteq\mathcal{S}^*_{\mathcal{D}}$ and worker $w_\ell\in\widetilde{\mathcal{W}}\subseteq\mathcal{S}^*_{\mathcal{W}}$, which means $\mathcal{H}(\mathcal{D}',\mathcal{W}')\leqslant\mathcal{H}(\emptyset,\emptyset)$ for any two sets $\mathcal{D}'\subseteq\mathcal{D}$ and $\mathcal{W}'\subseteq\mathcal{W}$, where $\emptyset$ is an empty set. Due to the choice of L, every worker or demander in $\mathcal{D}\cup\mathcal{W}$ can be observed independently with the probability ϕ. Similarly, each demander or worker in $\mathcal{D}\cup\mathcal{W}$ is not observed in the first L arrivals but belongs to the last R arrivals with probability $\min\{1,16\phi^{-1}\cdot\sqrt[3]{\eta}\}=16\phi^{-1}\cdot\sqrt[3]{\eta}$, independently. Thus, every worker $w_\ell\in\widetilde{W}$ or demander $d_i\in\widetilde{\mathcal{D}}$ belongs to $\widetilde{W}\backslash\mathcal{W}_L\cup\mathcal{W}_R$ or $\widetilde{D}\backslash\mathcal{D}_L\cup\mathcal{D}_R$ with probability $(1-\phi)(1-16\phi^{-1}\cdot\sqrt[3]{\eta})$. where η is the ratio parameter and ϕ is the selection probability. Therefore,

$$\begin{aligned}\mathbb{E}[\mathcal{H}(\mathcal{W}_L\cup\mathcal{W}_R,\mathcal{D}_L\cup\mathcal{D}_R)]&\geqslant(1-\phi-16\phi^{-1}\cdot\sqrt[3]{\eta}\\&\quad+16\sqrt[3]{\eta})\mathcal{H}(\emptyset,\emptyset),\end{aligned}\tag{13}$$

where $\emptyset$ means the empty set. With the help of Lemma 7, the expectation satisfies

$$\begin{aligned}\mathbb{E}[\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})]&\geqslant\Pr[\mathcal{E}]\mathbb{E}[\mathcal{H}(\mathcal{W}_L\cup\mathcal{W}_R,\mathcal{D}_L\cup\mathcal{D}_R)|\mathcal{E}]\\&\geqslant(1-\phi-16\phi^{-1}\cdot\sqrt[3]{\eta}+16\sqrt[3]{\eta})\cdot\mathcal{H}(\emptyset,\emptyset)-\Pr[\bar{\mathcal{E}}]\cdot\mathcal{H}(\emptyset,\emptyset)\\&\geqslant(1-\phi-16\phi^{-1}\cdot\sqrt[3]{\eta}+16\sqrt[3]{\eta}-\Pr[\bar{\mathcal{E}}])\cdot\mathcal{H}(\emptyset,\emptyset),\end{aligned}\tag{14}$$

where $\bar{\mathcal{E}}$ is the opposite of $\mathcal{E}$ defined in Lemma 6. Furthermore, $\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})$ is the social welfare achieved by CHASER over $\mathcal{S}_{\mathcal{D}\times\mathcal{W}}=\{(d_i,w_\ell)\in\mathcal{S}_{\mathcal{D}}\times\mathcal{S}_{\mathcal{W}}\mid w_\ell$ executes the task τ_i of $d_i\}$ with the winner sets $\mathcal{S}_{\mathcal{D}}\subseteq\mathcal{D}$ and $\mathcal{S}_{\mathcal{W}}\subseteq\mathcal{W}$. By Lemma 5, it has

$$\begin{aligned}\mathcal{H}(\emptyset,\emptyset)&=\sum_{d_i\in\widetilde{\mathcal{D}}}[v_i-\xi]+\sum_{w_\ell\in\widetilde{\mathcal{W}}}[\xi-c_\ell]\\&\geqslant(1-6\phi^{-1}\cdot\sqrt[3]{\eta})\cdot\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}),\end{aligned}\tag{15}$$

where $\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})$ is the social welfare over $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$. By setting $\phi=4\sqrt[6]{\eta}$, where $4\sqrt[6]{\eta}\leqslant 1/2$, since $\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})$ is optimal,

$$\begin{aligned}&\mathbb{E}[\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})]\geqslant(1-\phi-16\phi^{-1}\cdot\sqrt[3]{\eta}+16\sqrt[3]{\eta}-\Pr[\bar{\mathcal{E}}])\cdot\mathcal{H}(\emptyset,\emptyset)\\&\Rightarrow\frac{\mathbb{E}[\mathcal{U}(\mathcal{S}_{\mathcal{D}/\times\mathcal{W}})]}{\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})}\geqslant(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta}-10e^{-2/\sqrt[3]{\eta}})\\&\qquad\approx(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta}),\end{aligned}\tag{16}$$

where Eq. (16) holds since $10e^{-2/\sqrt[3]{\eta}}$ is negligible. □

As mentioned earlier, the BEMCS system aims to achieve high economic benefits in addition to maintaining anonymity and data confidentiality. However, the presence of fake information, including fake tasks and data, poses challenges to the system's efficiency and potential for economic gains. In contrast to existing incentive mechanisms that often focus on investigating worker costs or demander revenue separately, this paper takes a different approach by examining the social welfare of the entire system. By considering social welfare as the primary criterion, the proposed mechanism takes into account the collective well-being of both demanders and workers. It is important to note that higher social welfare typically implies higher demander revenue and lower worker costs, as indicated by its definition. This comprehensive perspective ensures that the proposed mechanism not only delivers better economic performance but also creates a balanced and favorable environment for all participants. By addressing the challenges posed by fake information, promoting efficiency, and maximizing economic benefits for all stakeholders, the mechanism presented in this paper offers a comprehensive solution that surpasses the limitations of previous works. It provides a framework that enhances the BEMCS system's economic performance while ensuring a fair and beneficial ecosystem for all involved.

Remark 3 The competitive ratio on social welfare is $\frac{\mathbb{E}[\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})]}{\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})}$ where $\mathcal{U}(\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}})$ is the optimal social welfare, while $\mathbb{E}[\mathcal{U}(\mathcal{S}_{\mathcal{D}\times\mathcal{W}})]$ is the expected social welfare achieved by our mechanism. Therefore, the ratio is closer to 1 means our mechanism has higher social welfare. As shown in Theorem 2, the ratio is lower bounded by $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta})$ which goes to 1 when $\eta\to 0$. It shows the sharpness of this bound. Furthermore, when our system model is assumed to

satisfy some other probability models, such as the Gaussian distribution and the Poisson distribution, the corresponding lower bound will be much sharper, which is investigated in our further works.

5.2 Security analysis

This subsection investigates the security properties of our designed BEMCS system with CHASER in smart contract, which is shown in Theorem 2. In fact the illustration of anonymity guaranteed by CHASER is illustrated in Fig. 2.

Data confidentiality: For the data confidentiality, the encrypted data and proofs generated by the zk-SNARK need to be considered. However, the confidentiality of encrypted data can be guaranteed by the asymmetric encryption, while that of the proofs can be guaranteed by the zero-knowledge of the zk-SNARK.

Anonymity: For the anonymity of workers and demanders, an adversary can break it in two ways: (i) link a worker or a demander via her blockchain address; (ii) link the collected data of a worker or the published task of a demander through her authenticating attestations. The first case is trivial since

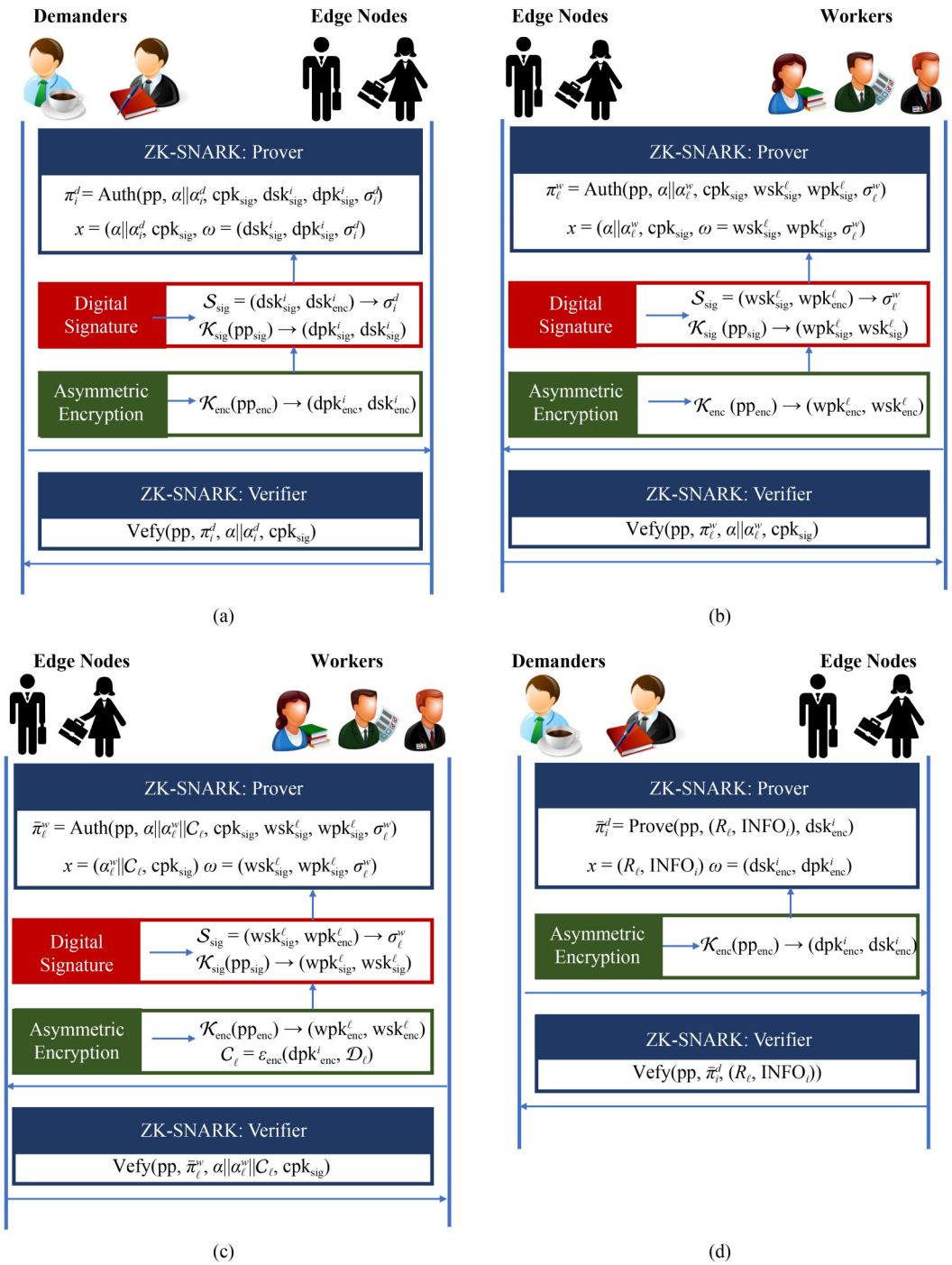

Fig. 2 (a) Anonymity authentication illustration of task publishing; (b) anonymity authentication illustration of parameter submission; (c) anonymity authentication illustration of data collection; (d) anonymity authentication illustration of payment transferring

each worker and demander utilizes a randomly created one-task-only address for a sensing task. The anonymity in the second case is guaranteed as follows.

Regarding the anonymity of workers and demanders, it requires us to guarantee that after observing the authentication transcripts of a worker or demander, the adversary can not distinguish whether a new authentication belongs to the identical participant. Since the adversary is not able to compute the secret key $\mathsf{wsk}_{\mathsf{sig}}^{\ell}$ or $\mathsf{dsk}_{\mathsf{sig}}^{i}$ from all public values, the tags $t_{w_\ell}^1$ and $t_{w_\ell}^2$ of worker w_ℓ as well as $t_{d_i}^1$ and $t_{d_i}^2$ of demander d_i computed in BEMCS systems can be regarded as some random values r. Therefore, the tags $t_{w_\ell}^1$, $t_{w_\ell}^2$, $t_{d_i}^1$, $t_{d_i}^2$ and the random values r can not be distinguished by the adversary. Because of the zero-knowledge of zk-SNARK, for a random value r, the adversary is able to control the common reference strings of zk-SNARK to generate a valid proof $\hat{\eta}$, which means that the tags $t_{w_\ell}^1$ and $t_{w_\ell}^2$ (similarly for $t_{d_i}^1$ and $t_{d_i}^2$) as well as the proof η_ℓ can be simulated by some random values r_1 and r_2 as well as a fake proof $\hat{\eta}$, respectively. However, all of the random values and the fake proof have nothing to do with the actual witness $\mathsf{wsk}_{\mathsf{sig}}^{\ell}$ or $\mathsf{dsk}_{\mathsf{sig}}^{i}$, which completes the discussion of the second case.

Security against the malicious demanders: The malicious demanders can obtain the benefits from two aspects: (i) disavow the policy broadcasted in the Task Publish; (ii) report a bid that deviates the actual value. The first threat is trivial since the SC is public and no one can deny the posted policy. The second is prevented since CHASER guarantees that each demander behaves truthfully.

Security against the malicious workers: The malicious workers can obtain the benefits from three aspects: (i) report a bid that deviates the actual cost; (ii) change the policy announced in the SC; (iii) copy other workers' collected data to earn some rewards. The first case is prevented since each worker is also truthful in CHASER. The second is trivial since the policy posted in the SC is immutable. The third can be prevented by the security of the digital signature scheme and the zk-SNARK. Combining the above analysis, the following theorem can be obtained.

Theorem 3 BEMCS system is data confidential, anonymous and secure against the malicious participants after applying the zk-SNARK property, asymmetric encryption and digital signature security, as well as incentive guarantee.

6 Performance evaluation

This section shows the simulation results of CHASER after introducing the evaluation rationale, testbed settings, baseline methods and simulation settings, which correspond to Subsections 1, 2, 3, 4 and 5, respectively.

6.1 Evaluation rationale

As discussed earlier, social welfare serves as a crucial metric for assessing the economic properties of incentive mechanisms, with higher social welfare typically corresponding to lower worker costs and higher demander revenues. The theoretical analysis conducted previously has demonstrated that CHASER achieves a high competitive ratio in terms of social welfare. Therefore, the evaluation in this study primarily focuses on examining the social welfare of CHASER through experimental simulations.

However, relying solely on social welfare may not provide a comprehensive understanding of CHASER's economic performance, as it does not consider the proximity to the optimal social welfare achievable by the system. To address this limitation, the evaluation in this section goes beyond assessing the achieved social welfare by also investigating the competitive ratio of CHASER's social welfare. This analysis aims to highlight the disparity between the experimental results, theoretical analysis, and the optimal outcomes.

The competitive ratio represents the gap between the achieved social welfare and the optimal values, where a smaller gap indicates better performance. By evaluating the competitive ratio, this study provides insights into how closely CHASER approaches the optimal social welfare. This additional perspective contributes to a more comprehensive understanding of CHASER's economic performance, showcasing its relative effectiveness in comparison to both the theoretical analysis and benchmarks.

6.2 Testbed settings

The simulation is implemented in our computer with Intel core i7-6700 CUP at 3.4 GHz, 8 GB of RAM running Microsoft Windows 10 64-bit version on 500 GB hard drive. The operation parameters of Blockchain are set according to Ethereum. The tools used for the whole simulation are MATLAB R2016a and Remix IDE of Ethereum.

6.3 Baseline methods

When evaluating the performance of incentive mechanism, three baseline methods are considered, which are conducted by utilizing the simulation settings in Table 1.

- *Price-Ranked Online Mechanism (PROM):* CHASER is compared to the Price-Ranked Online Mechanism (PROM) designed in [36], where all demanders and workers are strategic and selfish. In fact, although authors in [36] proposed four types of mechanisms based on the price function, CHASER is only compared with two of them.
  - *PROM-F:* The first is referred to as PROM-F, whose price function is a fixed constant.
  - *PROM-M:* The second is PROM-M, whose price is obtained by McAfee double auction.
- *Random Bidding Selection Mechanism (RBSM):* It is modified from CHASER. Unlike CHASER, a pair of worker and demander is selected randomly in the Standard Determination of RBSM without ordering to obtain the standard cost and value.

As demonstrated by CHASER, it operates as a threshold-based incentive mechanism in which demander-worker pairs are selected based on a pair of thresholds: the standard cost $\bar{c}$ and value $\bar{v}$. Workers with costs lower than $\bar{c}$ and demanders with values higher than $\bar{v}$ are chosen for task assignments. In the evaluation process, CHASER is initially compared to two

Table 1 Settings of parameter intervals for evaluating the performance of CHASER

Settings	Cost c_ℓ of worker	Value v_i of demander	Number M of demanders	Number W of workers	Ratio parameter η	Selection probability ϕ
I	$[5,20]$	$[15,30]$	$[200,380]$	400	0.005	0.5
II	$[5,20]$	$[15,30]$	800	$[300,800]$	0.003	0.5
III	$[5,30]$	$[10,15],[12,27],[15,20]$	350	$[180,360]$	0.002	0.5
IV	$[5,10],[7,12],[10,15]$	$[5,20]$	$[200,560]$	500	0.005	0.5
V	$[5,10]$	$[15,20]$	10^9	10^9	$[10^{-9},10^{-8}]$	$4\sqrt[6]{\eta}$
VI	$(0,10]$	$(10,20]$	$10^5,10^6,10^7,10^8$	$10^5,10^6,10^7,10^8$	$10^{-5},10^{-6},10^{-7},10^{-8}$	$[0.05,0.185]$

efficient threshold-based incentive mechanisms, namely PROM-F and PROM-M.

Additionally, it is evident that the effectiveness of CHASER relies on the determination of the standard value and cost. To investigate the impact of different approaches to standard determination, CHASER is compared to RBSM, where the standards are randomly selected.

6.4 Simulation settings

All parameters utilized for the simulations are listed in Table 1. In fact, the evaluation first varies the number M of demanders and the number W of workers from 200 to 380 and 300 to 800, respectively, to investigate the social welfare achieved by CHASER, where the cost c_ℓ of each worker w_ℓ and the value v_i of each demander d_i are sampled from the intervals $[5,20]$ and $[15,30]$, respectively, which are Setting I and Setting II in Table 1. The influences under different actual values v_i and costs c_ℓ on social welfare are studied by sampling them from $[10,15],[12,17],[15,20]$ and $[5,10],[7,12],[10,15]$, respectively, i.e., Settings III and IV in Table 1. In particular, in Settings I–IV, the selection probability ϕ is set to 0.5, while the ratio parameter η is less than 0.005.

As shown in Theorem 2, since the lower bound of competitive ratio has a nonintuitive form, to present the theoretical analysis of the corresponding lower bound achieved by CHASER, some large-scale scenarios are further considered in our simulations, which are also introduced in Setting V of Table 1. In fact, in Setting V, the ratio parameter η varies in the interval $[10^{-9},10^{-8}]$ and the selection probability ϕ also varies according to the equality $\phi = 4\sqrt[6]{\eta}$. It should be pointed out that such large scale scenarios shown in Setting V are practical since each data demander may publish many sensing tasks and each worker can execute more than one, where each sensing task results in a demander-worker pair.

Finally, as a BEMCS system, ensuring a high task completion rate is a crucial requirement. Therefore, the ratios in various scenarios are thoroughly investigated, as presented in Setting VI. The cost of each worker is chosen within the interval $(0,\frac{1}{2}]$,while the value of each demander falls within the range of $(10,20]$. Furthermore, the number of demander-worker pairs ranges from 10^5 to 10^8, resulting in corresponding values for the ratio parameter η. Finally, the selection probability ϕ is selected in $[0.05,0.185]$.

6.5 Simulation results

Figure 3(a) shows the cost in different numbers of demander-worker pairs. It can be observed that the increasing number leads to the increasing cost since more transactions need to be processed. Furthermore, Fig. 3(b) investigates the impact of the increasing transaction size. It shows that the large transactions cost more since they consume more resources from participants. The unit Gas is about 36 Gwei= 36×10^{-9} ETH, where ETH is Ethereum. Following the LONDON UPGRADE, the total `transaction fee` is determined by `units of gas used`$\times$(`base fee`+`priority fee`). The `base fee` is predetermined by the protocol, while the `priority fee` is a tip set by the demander for the edge nodes. The `base fee` is calculated using a formula that compares the size of the previous block (i.e., the total gas used for all transactions) with the target size. If the target block size is exceeded, the `base fee` may increase by a maximum of 12.5% per block. This exponential growth makes it

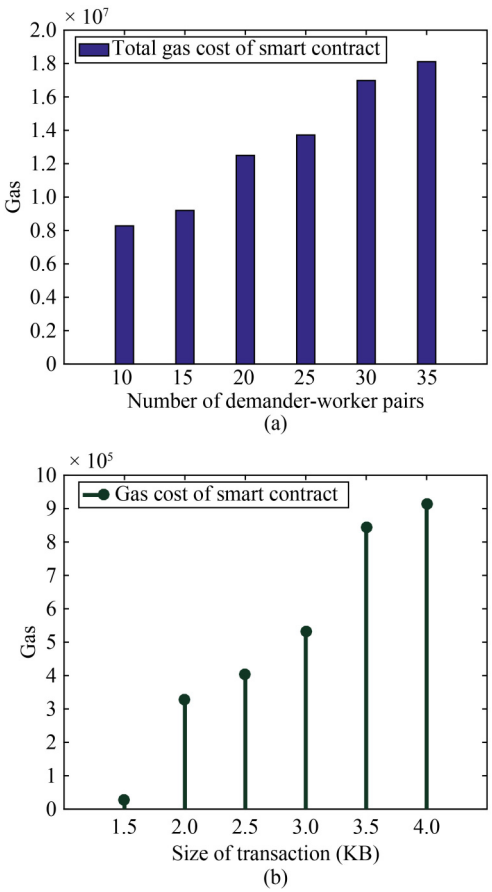

Fig. 3 (a) Gas cost of the smart contract versus different numbers of demander-worker pairs; (b) gas cost of the smart contract versus different sizes of transaction. The gas cost is paid for locking the transaction to the blockchain in Ethereum network

economically non-viable for block size to remain high indefinitely. Additionally, the gas required to support a smart contract is determined by the basic operations performed. For instance, the operation `ADD` consumes 3 Gas, while `MUL` requires 5 Gas. These gas costs reflect the computational complexity and resource consumption associated with each operation within the smart contract.

The social welfare with varying numbers of demanders is depicted in Fig. 4(a), with a fixed count of 400 workers. As the number of demanders increases, the social welfare also rises due to the allocation of more demanders with higher values. Notably, Fig. 4(a) demonstrates that when there are 380 demanders in the system, CHASER achieves a minimum of 100% increase in social welfare compared to the baseline mechanisms. Figure 4(b) illustrates the social welfare under different numbers of workers. Similar to the previous scenario, an increasing number of workers results in higher social welfare due to the selection of more workers with lower costs. It is noteworthy that Fig. 4 demonstrates a consistent trend of CHASER's welfare being approximately 42% higher in most cases.

As illustrated in Fig. 4, CHASER consistently achieves significantly higher social welfare compared to the baseline mechanisms. This notable performance can be attributed to several key factors

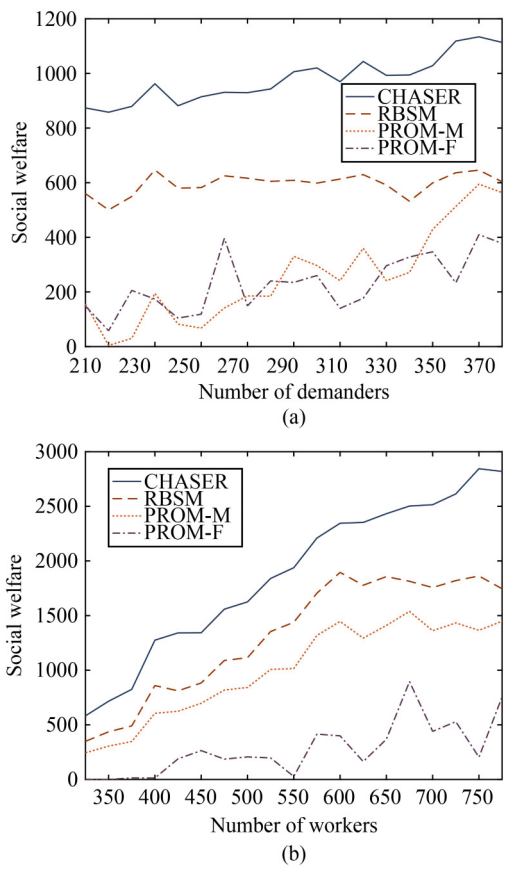

Fig. 4 (a) Social welfare versus different numbers of demanders, where the number of workers is 400; (b) social welfare versus different numbers of workers, where the number of demanders is 800. The cost and value are sampled in [5,20] and [15,30], respectively

- PROM-F utilizes a pre-supposed and fixed constant as the price function, neglecting the individual characteristics of workers and demanders. In contrast, CHASER determines payments based on the specific values and costs of participants. This personalized approach enables more accurate pricing and better matching of tasks with suitable participants, resulting in higher social welfare.
- PROM-M involves considering multiple conditions when matching workers and demanders, imposing stricter constraints and reducing the number of potential pairings. In contrast, CHASER adopts a more flexible and efficient matching process, allowing for a greater number of successful worker-demander pairs. This enhanced matching capability contributes to the higher social welfare achieved by CHASER.
- In RBSM, the standard value and standard cost are randomly selected, overlooking the individual characteristics of participants. Consequently, some participants may remain unallocated, leading to suboptimal social welfare. In contrast, CHASER adopts a systematic approach by ordering the values and costs and selecting standards accordingly. This systematic approach ensures a higher success rate in worker-demander allocations.

Figure 5 presents the social welfare achieved under varying values for each demander and different costs for each worker. In Fig. 5(a), with a fixed count of 350 demanders, the worker costs are sampled within the range of $[5,30]$, while in Fig. 5(b), with 500 workers, the demander values are sampled within the range of $[5,20]$. The figures demonstrate that higher values for demanders and lower costs for workers result in increased social welfare, as more successful worker-demander pairings can be selected. Additionally, Fig. 5 reveals that, while social welfare generally increases with the number of demanders and workers, there are some instances where the relationship is different. For instance, in Fig. 5(a), when there are 260 workers, the social welfare is lower than that when the number of workers is 240. This discrepancy can be attributed to the randomness inherent in the Standard Determination process of CHASER and the dynamic arrivals of participants. These factors introduce variations in the allocation outcomes and can lead to different levels of social welfare in certain scenarios. Figure 5 provides insights into the impact of demander values and worker costs on social welfare within the CHASER mechanism. It underscores the importance of appropriate values and costs to maximize social welfare, while acknowledging the influence of randomness and participant dynamics in the allocation process.

Figure 6(a) shows the gap among the theoretical analysis of lower bound, practical evaluation, and upper bound of competitive ratio. When the ratio parameter $\eta \leqslant 10^{-8}$, i.e., the numbers of demanders and workers are larger than 10^8, the theoretical lower bound is larger than 0.63. Furthermore, the lower bound decreases with increasing η, which matches the analysis of Eq. (16). Additionally, the practical evaluation also decreases with increasing η. This is because $\phi = 4\sqrt[6]{\eta}$ also

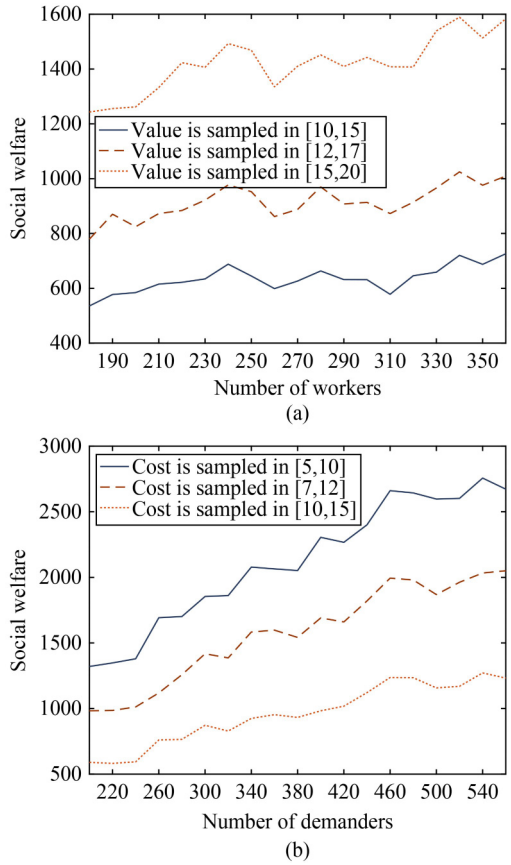

Fig. 5 (a) Social welfare versus different numbers of workers, where the number of demanders is 350 and the cost is sampled in [5,30]; (b) social welfare achieved by CHASER versus different numbers of demanders, where the number of workers is 500 and the value is sampled in [5,20]

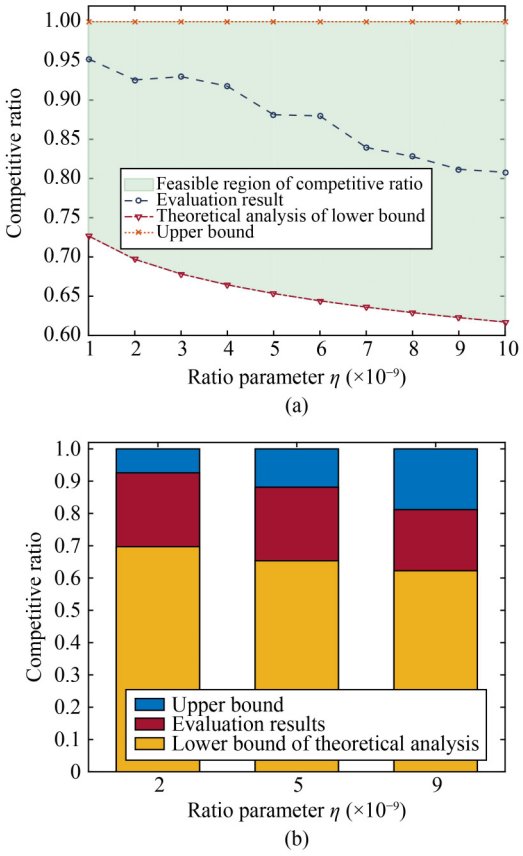

Fig. 6 Competitive ratio on social welfare versus different values of ratio parameter η, where the theoretical analysis of the lower bound is calculated by the right hand of Eq. (16)

increases with the increase in η, which means that more workers and demanders are selected in the Standard Determination to determine the standard value and standard cost, while fewer participants can be allocated in Winner Selection to execute the sensing tasks. It is worth noting that such large-scale scenarios are practical and relevant, as each demander has the ability to request multiple sensing tasks. In this context, each task corresponds to a demander-worker pair, amplifying the scale and complexity of the system. The practicality of these scenarios further underscores the significance of the evaluation results and their applicability to real-world settings.

Figure 6(b) shows some points under the corresponding parameters. When the ratio parameter $\eta = 9\times10^{-8}$, although the lower bound calculated by Eq. (16) is only 0.63, the evaluation results show that the ratio achieved by CHASER is approximately 0.8, which confirms its practical performance. Furthermore, it can be seen in Fig. 6 that the bound calculated by Eq. (16) is larger than $1-\frac{1}{e}\approx0.63$. Note that $1-\frac{1}{e}$ represents a significant benchmark achieved by many single-side incentive mechanisms [37].

As shown previously, the choice of selection probability ϕ and ratio parameter η has a significant impact on the task completion rate of CHASER. Therefore, Fig. 7 investigates the impact and gives the suggestion of selection. It is known that ϕ is selected in $(0,\frac{1}{2}]$ and η is selected in $(|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1},1]$. It can be seen that the values of η are related to the scale of system since it is lower bounded by $|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}$ where $\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}$ is the optimal matching set of the whole system. Furthermore, to implement CHASER, it requires the condition $\lceil(1-2\phi^{-1}\cdot\sqrt[3]{\eta})\cdot|\mathcal{S}^*_{\mathcal{D}_\mathcal{L}\times\mathcal{W}_\mathcal{L}}|\rceil>0$ holds in Algorithm 7. Therefore, Fig. 7 shows the corresponding selection of η and ϕ. It can be seen that with the decrease in η, the task completion rate increases. This is because that with the decreasing η, $1-2\phi^{-1}\cdot\sqrt[3]{\eta}$ increases, which means that the standard value $\bar{v}$ is smaller and the standard cost $\bar{c}$ is larger. Since Algorithm 8 only selects demanders whose bidding value v_i is larger than $\bar{v}$ and workers whose bidding cost c_ℓ is smaller than $\bar{c}$, more demander-worker pairs can be selected. Similarly, the increasing ϕ also leads to the increase in $1-2\phi^{-1}\cdot\sqrt[3]{\eta}$ at beginning, which results in the increase in the task completion rate. However, due to the increase in ϕ, the size L of observation queue Q increases, which means more demanders and workers are putted into Q whose tasks will not be executed. Therefore, the task completion rate finally decreases. Furthermore, since the value of η is lower bounded by $|\mathcal{S}^*_{\mathcal{D}\times\mathcal{W}}|^{-1}$, the system scale increases with the decreasing η. For example, when $\eta=10^{-8}$, it means that the number of whole demander-worker pairs in system needs at least 10^8. Hence, CHASER exhibits better performance in large-scale systems compared with the small-scale systems.

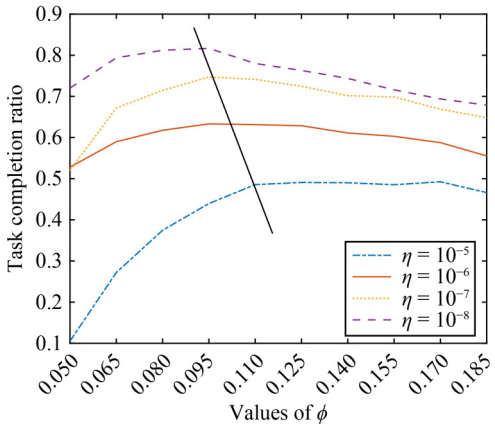

Fig. 7 Task completion rate versus different values of ratio parameter η and selection probability ϕ

7 Conclusion

This paper has proposed an incentive mechanism, namely, CHASER, by applying smart contracts after building a BEMCS system. It has been proved that CHASER guarantees the incentive requirements of double-side truthfulness, double-side individual rationality and budget balance for all demanders and workers. CHASER is $(1+28\sqrt[3]{\eta}-9.5\sqrt[6]{\eta}-24\sqrt[2]{\eta})$-competitive on social welfare. Moreover, the proposed BEMCS system with CHASER in smart contract has been proven to ensure the data confidentiality as well as anonymity, and also prevent the malicious participants from joining after applying the zk-SNARK property, asymmetric encryption and digital signature security as well as incentive guarantee. Finally, numerous extensive simulations have validated the desirable properties of CHASER.

Acknowledgement This work was supported in part by the Shanghai Science and Technology Innovation Action Plan (23511100400), and in part by the National Natural Science Foundation of China (Grants Nos. 62372288, and U20A20181), the 2023−2024 Open Project of Key Laboratory Ministry of Industry and Information Technology-Blockchain Technology and Data Security (20242216).

Competing interests The authors declare that they have no competing interests or financial conflicts to disclose.

References

1. Xiong J, Zhao M, Bhuiyan M Z A, Chen L, Tian Y. An AI-enabled three-party game framework for guaranteed data privacy in mobile edge crowdsensing of IoT. IEEE Transactions on Industrial Informatics, 2021, 17(2): 922–933
2. Fiore M, Nordio A, Chiasserini C F. Driving factors toward accurate mobile opportunistic sensing in urban environments. IEEE Transactions on Mobile Computing, 2016, 15(10): 2480–2493
3. Aitzhan N Z, Svetinovic D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 840–852
4. Tschorsch F, Scheuermann B. Bitcoin and beyond: a technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084–2123
5. Fiege U, Fiat A, Shamir A. Zero knowledge proofs of identity. In: Proceedings of the 9th Annual ACM Symposium on Theory of Computing. 1987, 210−217
6. Bitansky N, Canetti R, Chiesa A, Tromer E. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. 2012, 326−349
7. Liu M, Yu F R, Teng Y, Leung V C M, Song M. Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing. IEEE Transactions on Wireless Communications, 2019, 18(1): 695–708
8. Tang J, Tang H, Zhang X, Cumanan K, Chen G, Wong K K, Chambers J A. Energy minimization in D2D-assisted cache-enabled internet of things: a deep reinforcement learning approach. IEEE Transactions on Industrial Informatics, 2020, 16(8): 5412–5423
9. Jin H, Su L, Chen D, Guo H, Nahrstedt K, Xu J. Thanos: incentive mechanism with quality awareness for mobile crowd sensing. IEEE Transactions on Mobile Computing, 2019, 18(8): 1951–1964
10. Karaliopoulos M, Bakali E. Optimizing mobile crowdsensing platforms for boundedly rational users. IEEE Transactions on Mobile Computing, 2022, 21(4): 1305–1318
11. Li L, Yu X, Cai X, He X, Liu Y. Contract-theory-based incentive mechanism for federated learning in health crowdsensing. IEEE Internet of Things Journal, 2023, 10(5): 4475–4489
12. Wang Z, Li J, Hu J, Ren J, Wang Q, Li Z, Li Y. Towards privacy-driven truthful incentives for mobile crowdsensing under untrusted platform. IEEE Transactions on Mobile Computing, 2023, 22(2): 1198–1212
13. Xiao M, Xu Y, Zhou J, Wu J, Zhang S, Zheng J. AoI-aware incentive mechanism for mobile crowdsensing using stackelberg game. In: Proceedings of the IEEE Conference on Computer Communications. 2023, 1−10
14. Sun J, Jin H, Ding R, Fan G, Wei Y, Su L. Multi-objective order dispatch for urban crowd sensing with for-hire vehicles. In: Proceedings of the IEEE Conference on Computer Communications. 2023, 1−10
15. Li M, Weng J, Yang A, Lu W, Zhang Y, Hou L, Liu J N, Xiang Y, Deng R H. CrowdBC: a blockchain-based decentralized framework for crowdsourcing. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(6): 1251–1266
16. Chen X, Cheng Q, Yang W, Luo X. An anonymous authentication and secure data transmission scheme for the internet of things based on blockchain. Frontiers of Computer Science, 2024, 18(3): 183807
17. An J, Wu S, Gui X, He X, Zhang X. A blockchain-based framework for data quality in edge-computing-enabled crowdsensing. Frontiers of Computer Science, 2022, 17(4): 174503
18. Yu Y, Liu S, Guo L, Yeoh P L, Vucetic B, Li Y. CrowdR-FBC: a distributed fog-blockchains for mobile crowdsourcing reputation management. IEEE Internet of Things Journal, 2020, 7(9): 8722–8735
19. Zhang C, Guo Y, Jia X, Wang C, Du H. Enabling proxy-free privacy-preserving and federated crowdsourcing by using blockchain. IEEE Internet of Things Journal, 2021, 8(8): 6624–6636
20. Zhang C, Zhu L, Xu C, Sharif K. PRVB: Achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle. IEEE Transactions on Vehicular Technology, 2021, 70(1): 831–843
21. Mukkamala P S, Wu H, Düdder, B. Reliable and streaming truth discovery in blockchain-based crowdsourcing. In: Proceedings of the 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2023, 492−500
22. Yuan L, He Q, Chen F, Dou R, Jin H, Yang Y. PipeEdge: a trusted pipelining collaborative edge training based on blockchain. In: Proceedings of the ACM Web Conference. 2023, 3033−3043

23. Wang W, Wang Y, Duan P, Liu T, Tong X, Cai Z. A triple real-time trajectory privacy protection mechanism based on edge computing and blockchain in mobile crowdsourcing. IEEE Transactions on Mobile Computing, 2023, 22(10): 5625–5642
24. Hao M, Tan B, Wang S, Yu R, Liu R W, Yu L. Exploiting blockchain for dependable services in zero-trust vehicular networks. Frontiers of Computer Science, 2024, 18(2): 182805
25. Feng J, Yu F R, Pei Q, Du J, Zhu L. Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems. IEEE Transactions on Wireless Communications, 2020, 19(6): 4321–4334
26. Sun W, Liu J, Yue Y, Wang P. Joint resource allocation and incentive design for blockchain-based mobile edge computing. IEEE Transactions on Wireless Communications, 2020, 19(9): 6050–6064
27. Xiao L, Ding Y, Jiang D, Huang J, Wang D, Li J, Poor H V. A reinforcement learning and blockchain-based trust mechanism for edge networks. IEEE Transactions on Communications, 2020, 68(9): 5460–5470
28. Xu H, Huang W, Zhou Y, Yang D, Li M, Han Z. Edge computing resource allocation for unmanned aerial vehicle assisted mobile network with blockchain applications. IEEE Transactions on Wireless Communications, 2021, 20(5): 3107–3121
29. Jin Y, Jiao L, Qian Z, Zhou R, Pu L. Orchestrating blockchain with decentralized federated learning in edge networks. In: Proceedings of the 20th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2023, 483−491
30. Amiri M J, Lai Z, Patel L, Loo B T, Lo E, Zhou W. Saguaro: an edge computing-enabled hierarchical permissioned blockchain. In: Proceedings of the 39th IEEE International Conference on Data Engineering (ICDE). 2023, 259−272
31. Yuan L, He Q, Tan S, Li B, Yu J, Chen F, Yang Y. CoopEdge+: enabling decentralized, secure and cooperative multi-access edge computing based on blockchain. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(3): 894–908
32. Menezes A J, Van Oorschot P C, Vanstone S A. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1996
33. Sasson E B, Chiesa A, Garman C, Green M, Miers I, Tromer E, Virza M. Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings of 2014 IEEE Symposium on Security and Privacy. 2014, 459−474
34. Ying C, Jin H, Wang X, Luo Y. CHASTE: incentive mechanism in edge-assisted mobile crowdsensing. In: Proceedings of the 17th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON). 2020, 1−9
35. Feldman M, Frim G, Gonen R. Multi-sided advertising markets: dynamic mechanisms and incremental user compensations. In: Proceedings of the 9th International Conference on Decision and Game Theory for Security. 2018, 227−247
36. Wei Y, Zhu Y, Zhu H, Zhang Q, Xue G. Truthful online double auctions for dynamic mobile crowdsourcing. In: Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM). 2015, 2074−2082
37. Yang D, Xue G, Fang X, Tang J. Incentive mechanisms for crowdsensing: crowdsourcing with smartphones. IEEE/ACM Transactions on Networking, 2016, 24(3): 1732–1744

Chenhao Ying received the PhD degree in the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China in 2022. He is currently a research assistant professor in the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His current research interests include mobile crowd sensing, blockchain, and mobile computing.

Haiming Jin is currently a tenure-track associate professor in the Department of Computer Science and Engineering at Shanghai Jiao Tong University, China. He is interested in addressing unfolding research challenges in the general areas of urban computing, cyber-physical systems, crowd and social sensing systems, network economics and game theory, reinforcement learning, and mobile pervasive and ubiquitous computing.

Jie Li received the BE degree in computer science from Zhejiang University, China, the ME degree in electronic engineering and communication systems from China Academy of Posts and Telecommunications, China, and the Dr Eng degree from the University of Electro-Communications, Japan. He is currently a chair professor in Department of Computer Science and Engineering, the director of SJTU Blockchain Research Centre, Shanghai Jiao Tong University, China. His research interests include Big Data and AI, blockchain, network systems, and security. He was a full professor at the Department of Computer Science, University of Tsukuba, Japan. He is the co-chair of IEEE Technical Community on Big Data and the founding Chair of IEEE ComSoc Technical Committee on Big Data and the cochair of IEEE Big Data Community. He serves as an associated editor for many IEEE journals and transactions. He has also served on the program committees for several international conferences.

Xueming Si is the director of Frontier Information Technology Research Institute of Zhongyuan University of Technology, China. He is currently the director of the Blockchain Special Committee of the China Computer Federation. His research interests are cryptography, data science, computer architecture, network and information system security, and blockchain.

Yuan Luo received the BS degree in applied mathematics and the MS and PhD degrees in probability statistics from Nankai University, China in 1993, 1996, and 1999, respectively. Since 2006, he has been a full professor with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests include coding theory, information theory, and big data analysis.